IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 18 September 2023, accepted 17 October 2023, date of publication 23 October 2023, date of current version 10 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3327016

RESEARCH ARTICLE

Cyber Threats Classifications and Countermeasures in Banking and Financial Sector

ABDULBASIT A. DAREM[1], (Member, IEEE), ASMA A. ALHASHMI[1], TAREQ M. ALKHALDI[2], ABDULLAH M. ALASHJAEE[3], SULTAN M. ALANAZI[1], AND SHOUKI A. EBAD[1]

[1]Department of Computer Science, Northern Border University, Arar 73213, Saudi Arabia
[2]Department of Educational Technologies, Imam Abdulrahman Bin Faisal University, Dammam 34221, Saudi Arabia
[3]Department of Computer Sciences, Faculty of Computing and Information Technology, Northern Border University, Rafha 91911, Saudi Arabia

Corresponding author: Abdulbasit A. Darem (basit.darem@nbu.edu.sa)

This work was supported by the Deanship of Scientific Research, Northern Border University, Arar, Saudi Arabia, under Grant RG-NBU-2022-1724.

ABSTRACT The banking and financial sector has always been a prime target for cyber threats due to the critical nature of the information they handle. With the increasing dependence on technology and digital transformation, the sector is facing more complex and sophisticated threats from cybercriminals. The banking sector serves as the backbone of a country's economy, interlinked with various other sectors like petroleum, mining, health, and industry. Any significant damage to the banking sector can send shockwaves through the entire economic landscape. Therefore, cyber threat classifications play a crucial role in risk management and provide a valuable framework for understanding and responding to cyber threats. Understanding the potential impact of a cyber-attack helps organisations assess the risks they face and develop appropriate risk mitigation strategies. The purpose of this research paper is to provide a comprehensive analysis of cyber threats in the banking and financial sectors, including identifying common threats, their nature and character to help in classification. One of the significant contributions of this research paper is to classify cyber threats to the banking and financial sectors based on their severity and technicality. This classification helps to identify the appropriate countermeasures required to mitigate the risks of each type of threat. Furthermore, the paper explores the technical, non-technical, organizational countermeasures and the legal and regulatory measures used to protect financial transactions from cyber threats. This research work delves into the challenges and limitations of cyber threat classifications, focusing specifically on those confronting the banking and financial sector in their pursuit of robust cybersecurity. Additionally, it analyses recent trends and developments in the field, highlighting the evolving nature of cyber threats to banking. The most significant challenge is the rapidly evolving nature of cyber threats, making it challenging to keep up with the latest trends and technologies.

INDEX TERMS Cyber threats, banking and financial sector, threat classification, risk management, cyber attacks, countermeasures.

I. INTRODUCTION

The banking and financial sector is a critical infrastructure that plays a crucial role in the global economy. The sector has undergone a significant transformation in the last decade, with technological advancements leading to the digitisation of banking services. As a result, the sector has become more dependent on technology, and this has brought about new challenges and risks. Cybersecurity is one of the most significant challenges facing the banking industry today [16], [17], with cyber threats becoming more sophisticated and frequent. Cyber threats in the banking sector can have a significant impact, including financial loss, reputation damage, and legal consequences. Therefore, it is essential to understand the nature and character of these threats and develop effective countermeasures to mitigate their impact [19]. However, the

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

digitisation of banking services has brought about many benefits, including increased accessibility, convenience, and efficiency, and has also made the sector more vulnerable to cyber threats. The increasing use of online banking, mobile banking, and other digital services has created new avenues for cybercriminals to exploit [20], [21]. In addition, hackers have become more advanced in technology, making it challenging for banks to stop cyber threats at the same time. Cybercrimes have become very prevalent in the financial sector, and it is now believed to be one of the industry's greatest risks. Cybercriminals are constantly devising new methods of attack, and the banking sector must keep up with these evolving threats to protect itself and its customers.

There have been several instances of cyberattacks on banks and financial institutions in recent years. Some examples include a ransomware attack on Flagstar Bank in the USA in 2020, a DDoS attack on a network provider that forced the New Zealand Stock Exchange to shut down operations in 2020, and a data breach on the online stock trading platform Robinhood in 2021 where the personal information of 7 million customers was accessed by a cybercriminal [92]. The impact of cyber-attacks on the banking industry can be severe, including financial loss, reputational damage, and legal liabilities. For example, a recent report revealed that the average cost of a data breach was USD 3.86 million in 2020 [8]. Furthermore, the number of ransomware attacks worldwide increased by 148% between February and March 2020, while phishing attacks increased by 510% between January and February 2020 [9]. In the baseline case, some other reports stated that average losses due to cyberattacks for countries are around $97 billion or 9 percent of bank net income [34]. In the severe scenario-where the frequency of events is twice the peak observed in 2013-average losses would amount to USD 268 billion (26 percent of net income) and risk indicators would range between USD 352 and 539 billion (34 to 52 percent of net income) [34]. According to a report by Fortunately, the cost of cyber-attacks on banks reached $18.3 million in 2021. The potential economic damage from a cyberattack on the financial sector is significant, with estimates ranging from $50 billion to $120 billion [15]. Financial institutions are 300 times more likely to experience cyberattacks than other institutions, and the risk of bank failure from a major cyberattack is not far-fetched [10]. Cyber-attacks can also lead to losses of up to $100 billion for financial institutions [13]. Therefore, it is crucial for banks to take cybersecurity seriously and implement effective measures to protect their data and systems [11].

The banking and financial sectors require robust cybersecurity measures due to the myriad of cyber threats that have evolved over the years. Therefore, detecting and mitigating cyber threats in the banking sector requires a comprehensive approach that involves a combination of methods, techniques, workflow, and tools [16]. Methods and techniques include intrusion detection and prevention systems, antivirus software, firewalls, network security monitoring, and security information and event management systems. The workflow involves identifying and prioritising threats, analysing their impact, and developing appropriate response plans. Understanding and addressing the complex landscape of cyber threats is critical to ensuring the security and stability of these essential institutions. By examining the various types of cyber threat and their consequences, along with the technical, legal, and organisational countermeasures that can be implemented, this research aims to provide a comprehensive overview of the current state of cybersecurity in the banking sector and contribute to the development of more effective strategies and solutions for protecting against cyber threats. This research seeks to answer the following questions.

- What are the common cyber threats faced by the banking and financial sector and how can these threats be classified based on their severity and technicality?
- What are the specific technical, nontechnical, and organisational countermeasures that can effectively mitigate the risks of each type of cyber threat in the banking and financial sector?

This paper is organized as follows: The Introduction outlines the research problem and its relevance in the field of cyberbullying. The 'Literature Review' section reviews existing research and identifies gaps. The 'Recent Trends and Developments' section discusses current trends in cyberbullying. The 'Characteristics of Cyberbullying' section explores specific characteristics of cyberbullying. The 'Taxonomy of Cyberbullying' section presents a comprehensive taxonomy of cyberbullying. The 'Cyberbullying Classification' section analyzes different types of cyberbullying. The 'Challenges and Limitations' section discusses the challenges in addressing cyberbullying. The 'Implications and Recommendations' section presents recommendations for future research. Finally, the 'Conclusions' section summarizes the research findings and their implications.

II. LITERATURE SURVEY

Several studies have been conducted to identify and classify cyber threats in the banking and financial sectors. Shkodinsky [12] conducted a critical review of the domestic and foreign scientific literature and practical recommendations to ensure the protection of the banking institution from cyber threats in the digital economy. Yevseiev et al. [27]. proposed an advanced classification of threats to bank information resources. Tsvetanova and Stefanova [28] presented popular cyber threats targeting the financial and banking sectors. Best et al. [39]. made a comparative analysis of the most common threats to the banking sector based on bank reports and cybersecurity companies. Boitan [97] classified cyber-attacks into four main categories and emphasised that any attack on the critical components or services of the financial system could threaten the stability of the financial system or the financial security of its participants. Nobles [98] highlighted the vulnerability of the financial industry to sophisticated cybersecurity threats, human factors, social engineering, credit card fraud, and online banking schemes. Jakovljevi [100]

identified mobile applications and Web portals as the most significant sources of cyber threats in the banking industry. To counter these threats, various countermeasures have been proposed. Dubois and Tatar [99] discussed the importance of training and test beds to better prepare against cyber threats. Al-Alawi and Al-Bassam [101] proposed a combination of recommended factors as factors relating to cybersecurity awareness in the banking sector. Other literature classified cyber threats as targeted or non-targeted [91], external, or internal [42]. Targeted attacks are usually directed at specific organisations or individuals and are typically carried out by experienced cybercriminals. Nontargeted attacks, on the other hand, are aimed at any vulnerable system and are often carried out by less experienced attackers using off-the-shelf attack tools. External threats are usually caused by hackers that attempt to breach the security of the banking system. Internal threats, on the other hand, are caused by employees, contractors, or partners who have authorized access to the system.

Ali et al. [102] critically analyzed and discussed the effects of cyber threats when dealing with online banking services. Lin and Wang [103] highlighted the growing cyber threat that has created an uncontrollable financial mess for the global banking industry. Al- Somogyi and Nagy [104] observed an increasing trend in the number of cyberattacks in the banking industry, which demonstrates the importance of information security in this sector. Many literatures classified cyber threats in the banking sector into many groups [22] like malware, phishing, distributed denial of service (DDoS), and insider threats. Malware is a type of malicious software designed to infiltrate a system and disrupt its operations [23]. Malware can be used to steal sensitive information, such as user credentials, banking details, and personal information. Phishing is a type of attack that involves sending fraudulent emails or creating fake websites to trick users into divulging sensitive information. Phishing attacks can be highly sophisticated and difficult to detect, and often rely on social engineering to manipulate victims into revealing information [24], [30]. DDoS attacks are designed to overload a system with traffic to disrupt its operations [26]. DDoS attacks can be targeted at specific organizations or systems or can be nontargeted attacks that affect any vulnerable system. Insider threats involve employees, contractors, or partners who misuse their access privileges to steal or damage data. Other key threats include vulnerability exploitation attacks, trojans, ransomware, spoofing, SQL injections, local file inclusion, and cross-site scripting [4], [5], [6], [7].

Zahoor et al. [30] delves into this emerging crisis, meticulously analysing the various challenges that banks face in an increasingly digitized landscape. His work underscores the importance of identifying the security mechanisms currently employed by banks and suggests countermeasures to foster a safer banking environment. However, it also raises fundamental questions about the adequacy of existing security practises and the need for innovative solutions to address evolving threats. Complementing Zahoor's work, Sheehan et al. [33] challenge the sufficiency of traditional qualitative methods for assessing cyber risk. They propose a comprehensive set of criteria that include threat actors, threat events, vulnerabilities, safeguards, and consequences. It offers a promising direction for quantifying cyber risk, enabling more effective risk mitigation strategies. To further improve our understanding of cyber risk, Bouveret [34] and Kaffenberger and Kopp [32] each provide frameworks for the assessment of cyber risk. Bouveret explores different types of cyber incidents, such as data breaches, fraud, and business disruption, and identifies patterns of cyberattacks. His quantitative framework offers a tractable tool for institutions and supervisors to assess cyber risk in the financial sector. Kaffenberger and Kopp, on the other hand, broaden the scope of analysis to the national level. Their conceptual framework presents a method for assessing systemic cyber risk by analysing cyber risk exposures, assessing cybersecurity and preparedness capabilities, and identifying buffers available to absorb cyber-risk-induced shocks. On the strategic front, Akinbowale et al. [36] introduce the Balanced Scorecard (BSC) as a strategic management tool to mitigate cyber fraud. Their approach stands out in its emphasis on the importance of nonfinancial measures in the banking sector's cyber fraud mitigation efforts. Highlights the need to consider a broader range of factors, beyond financial metrics, when formulating effective cybersecurity strategies. However, the prevention of cyberattacks is not solely the responsibility of banks. Varga et al. [36] argue that a common operational picture is essential for effective awareness of cyber situations and risk management. Their study of the Swedish financial sector found that despite having a well-developed crisis management concept, there's a systemic failure to collect, analyze, and utilize information about rational adversaries causing prolonged disturbances. This gap underscores the need for better data utilization and the integration of such data into the sector's crisis management frameworks. Complementing the perspective of Varga et al. [36], Kiwia et al. [38] offer a granular understanding of cyber threats through their proposed taxonomy of banking Trojans. This threat intelligence-based taxonomy provides a stage-by-stage operational understanding of a cyber-attack and can be instrumental for security practitioners in designing effective detection and mitigation strategies. Navigating the realm of systemic cyber risks, Doerr et al. [41] and Crisanto et al. [73] tackle the issues from the viewpoint of central banks and regulatory bodies, respectively. They reveal the intensified focus on technical security control and resiliency and underscore the need for regulatory authorities to adopt a risk-based approach to enhance banks' cyber-security frameworks. Collectively, these studies weave a comprehensive tapestry of the current state of cyber security in the banking sector, elucidating its many facets. However, gaps remain to be in depth explored, particularly in the realms of threats classifications and countermeasures, indicating rich avenues for future research.

III. RESEARCH DESIGN AND FRAMEWORK DEVELOPMENT

This section outlines the research design adopted to develop a framework for Cyber Threats Classifications and Countermeasures in the Banking and Financial Sector. The design process followed [105] which incorporates various steps to identify key components, define criteria for classification, explore threat intelligence sources, develop a taxonomy, determine granularity, assign threat severity levels, or risk scores, and continuously assess and refine the framework based on feedback, real-world incidents, and threat landscape updates.

The framework development process involves a series of iterative steps, including identifying key components, defining classification criteria, exploring threat intelligence sources, developing a taxonomy, determining granularity, and assigning threat severity levels or risk scores. Each step is guided by the literature review findings. The framework will be designed to be comprehensive, practical, and adaptable to the unique characteristics of the Banking and Financial Sector. FIGURE 1 shows the framework development process, which comprises the following steps:

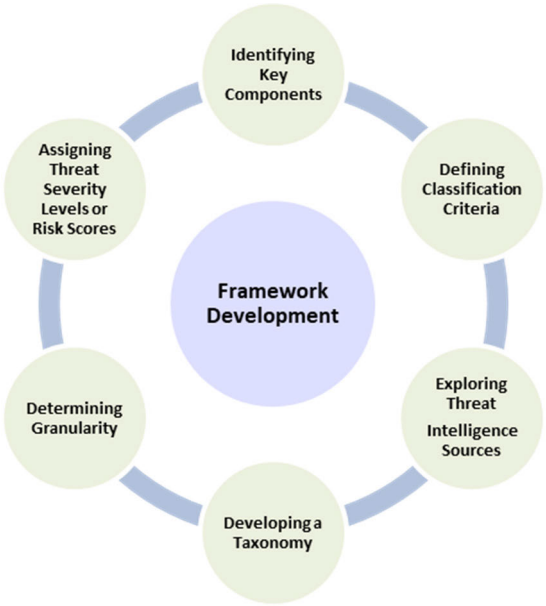

FIGURE 1. Framework development.

A. IDENTIFYING KEY COMPONENTS

The initial step in the framework development process involves identifying the key components that form the basis of the framework. This is achieved through an extensive review of existing frameworks, drawing upon scholarly literature, industry reports, and best practices in the field. The identified components may include threat categories, attack vectors, vulnerability types, impact factors, and mitigation strategies.

B. DEFINING CLASSIFICATION CRITERIA

Once the key components are identified, the subsequent step is to define the classification criteria. These criteria establish a set of attributes or characteristics that enable the categorization of cyber threats within the framework. The classification criteria are designed to be specific, measurable, and aligned with the research objectives. They serve as a foundation for effectively classifying threats based on their distinct characteristics, potential impact, and relevance to the Banking and Financial Sector.

C. EXPLORING THREAT INTELLIGENCE SOURCES

Enhancing the framework's effectiveness requires exploration of various threat intelligence sources and data feeds. This step entails evaluating a range of external sources, such as threat intelligence platforms, security vendors, government agencies, and industry-specific information sharing groups. These sources provide valuable insights into emerging threats, attack trends, and indicators of compromise. By leveraging diverse threat intelligence sources, the framework can capture a comprehensive view of the threat landscape in the Banking and Financial Sector.

D. DEVELOPING A TAXONOMY

This step involves creating a logical and coherent arrangement of threat categories, subcategories, and associated attributes within the framework. Taxonomy should provide a flexible framework that can accommodate new threat types and evolving attack techniques, while maintaining consistency and clarity in the classification process.

E. DETERMINING GRANULARITY

This step involves establishing the level of detail at which threats should be classified. The granularity should be based on the specific needs and capabilities of the Banking and Financial Sector, considering resource constraints, the complexity of the threat landscape, and the requirements of decision-making processes.

F. ASSIGNING THREAT SEVERITY LEVELS OR RISK SCORES

To effectively prioritize response efforts and allocate resources, a robust process for assigning threat severity levels or risk scores is integrated into the framework. This step entails defining a set of criteria and measurement scales to assess the potential impact, likelihood of occurrence, and overall risk associated with each identified threat category. The process adheres to principles of consistency, transparency, and alignment with industry standards or established risk management frameworks.

The framework development process is iterative, allowing for continuous refinement and improvement. As new threats emerge, lessons are learned from real-world incidents, and updates in the threat landscape occur, the framework will be adapted and updated to maintain its relevance and

effectiveness in addressing cyber threats in the dynamic context of the Banking and Financial Sector.

IV. CYBER THREATS FRAMEWORK

FIGURE 2 outlines the various parts of the framework in this section. Additionally, issues including the nature, character, and classification criteria for cyber threats will be covered.

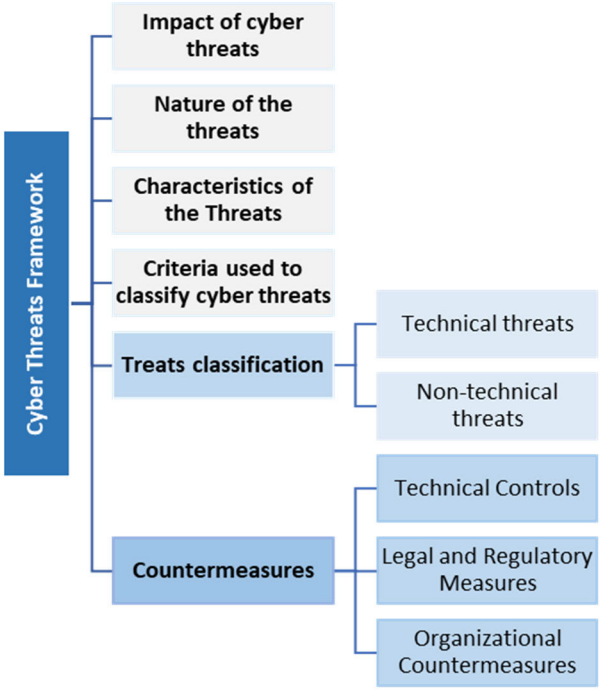

FIGURE 2. Cyber threats framework.

A. IMPACT OF CYBER THREATS

Cyber threats can have significant impacts on the banking and financial sectors, due to the sensitivity and confidentiality of financial information posing risks to the stability, security, and integrity of these institutions. Understanding the impact of cyber threats is crucial for comprehending the potential consequences and implications they pose to the Banking and Financial Sector. In this section, we delve into an analysis of the impact of cyber threats, examining the various dimensions that encompass their potential effects. Through a meticulous process of organization, we have classified the impact of cyber threats into distinct categories, providing a comprehensive framework that elucidates the potential ramifications faced by the sector. The process of organizing the impact of cyber threats involved a systematic evaluation of the potential consequences across multiple dimensions. We considered the immediate and direct impact on critical infrastructure, financial loss, and disruption to operations. Additionally, we explored the secondary and indirect effects, such as reputational damage, loss of customer trust, legal and regulatory consequences, and long-term financial implications.

The classification of impact was achieved through a comprehensive analysis of real-world incidents, expert opinions, and relevant industry reports. By synthesizing these diverse sources of information, we were able to identify and categorize the impact into key areas. These areas include financial impact, operational impact, reputational impact, regulatory impact, and legal impact. Each impact category is accompanied by a detailed description, highlighting the potential consequences and significance within the Banking and Financial Sector. This approach not only provides a comprehensive understanding of the impact but also enables stakeholders to prioritize their mitigation efforts and allocate resources effectively. Organizing the impact of cyber threats in a structured manner, to enhance the sector's ability to assess and manage the risks associated with these threats. Recognizing the multifaceted nature of their impact allows organizations to develop robust incident response plans, establish effective risk management strategies, and implement targeted measures to mitigate the potential consequences. TABLE 1 shows the ranking of some of the key impacts of cyber threats. The ranking is based on the potential severity and general implications. The threat to financial stability is considered the most severe as it could impair the solvency of a financial institution and have a spillover effect on other banks. Financial losses and reputational damage are also considered serious impacts of cyber threats on banking and financial services. Data breaches, operational disruption, compliance and regulatory issues, and increased costs are other impacts that can negatively affect the operations and reputation of banking and financial services. Competitive disadvantage is considered the least severe impact as it does not necessarily affect the financial stability of a financial institution.

B. THE NATURE OF THE THREATS

It is essential to comprehend the nature of cyber dangers in order to develop efficient techniques for their detection, prevention, and mitigation. In this subsection, we explore an in-depth analysis of the characteristics and attributes that define the nature of cyber threats. By following a meticulous process, we have examined and categorized the various dimensions that encompass the nature of these threats, providing a comprehensive framework to enhance our understanding and response to cyber risks. Through this process, we have categorized the nature of cyber threats into distinct dimensions. These dimensions include the technical sophistication of attacks, the level of persistence exhibited by threat actors, the range of targets and sectors affected, and the motives driving cybercriminal activities. By examining these dimensions, we aim to provide a comprehensive understanding of the diverse nature of cyber threats faced by the Banking and Financial Sector. Each dimension is accompanied by a detailed description that captures its significance and implications within the sector.

TABLE 2 lists the ranking of the nature of the threats and the description of each threat's nature. The ranking is based on the general implications and potential severity of the nature of threats on banking and financial services. The adversarial nature of cyber threats is considered the most

TABLE 1. Summarize some of the key impacts of CYBER threats in banking and financial sectors.

Cyber Threats' Impact	Description
Threat to financial stability [31][33]	Large-scale cyberattacks on critical financial infrastructure or multiple institutions can pose systemic risks to the entire financial sector. This can lead to reduced confidence in the financial system, destabilization of markets, and economic repercussions on a regional or global scale.
Financial losses [29]	Cyberattacks can result in financial losses through theft, fraud, or ransomware attacks. This can include unauthorized access to funds, fraudulent transactions, or demands for ransom to restore access to compromised systems.
Reputational damage[31]	Security breaches can damage the reputation of financial institutions, leading to loss of customer trust and potential loss of business. Customers may choose to move their accounts to other institutions, and it can be challenging to rebuild trust after an incident.
Data breaches [31][32][25]	Cyber threats can result in unauthorized access to sensitive data, such as personal information, transaction details, and intellectual property. Data breaches can lead to identity theft, financial fraud, and other criminal activities, as well as increased regulatory scrutiny and potential legal liabilities.
Operational disruption [32]	Cyberattacks can disrupt the normal functioning of financial institutions by causing system outages, service interruptions, or damage to critical infrastructure. This can lead to delays in processing transactions, customer service issues, and potential regulatory penalties.
Compliance and regulatory issues [31][33]	Cyberattacks can expose weaknesses in compliance and trigger increased regulatory scrutiny, leading to fines, penalties, and additional requirements.
Increased costs [31][33]	These costs include technology upgrades, employee training, and incident response management, among others. In the aftermath of a cyberattack, organizations may also face legal fees, compensation claims, and costs associated with rebuilding their reputation.
Competitive disadvantage [30]	Financial institutions that fail to adequately protect against cyber threats may find themselves at a competitive disadvantage, as customers and partners may prefer to work with more secure organizations.

TABLE 2. The nature of the threat's dimensions with description.

Dimensions	Description
Adversarial nature of cyber threats [38]	Organized crime syndicates, nation-states, or state-sponsored groups often perpetrate cyber threats targeting the banking sector. These adversaries possess the resources, expertise, and motivation to execute sophisticated attacks. Their tactics may include social engineering to manipulate employees, exploiting software or hardware vulnerabilities, and using advanced persistent threats (APTs). The adversarial nature of these threats makes it difficult to defend against such attacks.
Rapidly evolving character of cyber threats [38]	As technology advances, cybercriminals continually adapt and develop new methods to exploit vulnerabilities and gain access to sensitive information. The emergence of mobile banking and digital payments has created additional opportunities for attackers to target the banking sector.
Covert nature of cyber threats [38][36]	Cyber threats are often hidden and difficult to detect, enabling attackers to operate unnoticed for extended periods. They may use various techniques to mask their activities, such as disguising malware as legitimate software or using encryption to hide stolen data. This covert nature poses significant challenges in identifying and defending against these threats.
Collaboration in addressing cyber threats [40]	Addressing the complex nature and character of cyber threats requires a collaborative approach among various stakeholders. Banks must work with government agencies, technology companies, and other financial institutions to identify new threats and vulnerabilities, develop innovative technologies and best practices, and share information about cyber threats. This collaboration is essential for staying ahead of cybercriminals and mitigating the risks posed by cyber threats to the banking sector.
Impact of cyber threats on banking [38][31]	Cyber threats can have severe consequences for the banking sector, including financial losses, reputational damage, legal liabilities, and the theft of sensitive information, such as customer data and financial records. The loss of this information can lead to identity theft, fraud, and other criminal activities, further underscoring the importance of robust cybersecurity measures.

severe as cybercriminals intentionally target banking and financial services to gain financial benefits. Rapidly evolving character of cyber threats is also considered serious as cybercriminals frequently update their tactics and techniques to bypass cybersecurity measures. The covert nature of cyber threats is another nature that poses a risk to banking and financial services as cybercriminals may remain undetected for a long time. Collaboration in addressing cyber threats is crucial as it helps to mitigate the risks of cyber threats by sharing knowledge and resources. Impact of cyber threats on banking is considered the least severe nature of threats as it is a consequence of other natures of threats, such as financial losses and reputational damage.

C. THE CHARACTERISTICS OF THE THREATS

The character of cyber threats refers to the attributes, motivations, and goals of the threat actors involved. Understanding these characteristics can help institutions better prepare for and respond to cyber threats. The ranking of the main characteristics of cyber risks in the banking and financial sectors is shown in TABLE 3. The character of cyber threats plays a critical role in understanding their behavior, capabilities, and potential impact. In this section, we delve into a comprehensive analysis of the character of cyber threats, exploring the distinct attributes and traits that define their nature. By following a rigorous process, we have examined and categorized the key characteristics that shape the character of these threats, providing a framework to enhance our understanding and response to cyber risks. Through this process, we have categorized the character of cyber threats into distinct dimensions. These dimensions include the level of sophistication displayed by threat actors, the complexity of attack techniques employed, the degree of organization and coordination among threat groups, and the adaptability and agility demonstrated by cybercriminals. By examining these dimensions, we aim to provide a comprehensive understanding of the

diverse character of cyber threats encountered within the Banking and Financial Sector. Each dimension is accompanied by a detailed description that sheds light on its significance and implications within the sector.

The ranking is based on the factors of motivation, sophistication, persistence, adaptability, collaboration, geographical distribution, target selection, insider involvement, multi-vector attacks, and use of legitimate software or tools. Insider involvement is considered the most impactful threat to banking and financial services as it poses a risk to sensitive data and financial transactions. Multi-vector attacks and sophistication are also considered serious threats as cybercriminals use multiple attack vectors and advanced techniques to bypass cybersecurity measures. The use of legitimate software or tools is another threat that can make it difficult to detect and prevent cyber-attacks. Adaptability, persistence, geographical distribution, target selection, collaboration, and motivations are other factors that can impact the character of threats on banking and financial services.

TABLE 3. Threats' characteristics.

Characteristics	Description
Insider involvement [41]	Cyber threats can involve insider collaboration, with threat actors recruiting or manipulating employees or other insiders with access to sensitive information or systems.
Multi-vector attacks [43]	Attackers may employ multiple attack vectors simultaneously, such as combining phishing, malware, and DDoS attacks, to increase the likelihood of success and overwhelm an organization's defenses.
Sophistication [41]	The level of sophistication in cyber threats can vary greatly, ranging from low-skilled hackers and script kiddies to highly organized and well-funded criminal syndicates or nation-state sponsored groups.
Use of legitimate software or tools [41]	Some cyber threat actors use legitimate tools and services, such as cloud storage or software development platforms, to obfuscate their activities and evade detection.
Adaptability [25]	Cybercriminals continuously adapt their tactics, techniques, and procedures (TTPs) to evade detection and exploit new vulnerabilities. This requires financial institutions to constantly update and refine their cybersecurity measures.
Persistence [41]	Some cyber threats, such as Advanced Persistent Threats (APTs), involve long-term, stealthy campaigns that infiltrate and monitor financial systems for extended periods before initiating an attack.
Geographical distribution [42]	Cyber threats to the banking and financial sector can originate from anywhere in the world, as cybercriminals take advantage of global connectivity and differences in legal jurisdictions to evade law enforcement.
Target selection [43][91]	Cyber threat actors may target specific institutions based on factors such as perceived vulnerability, potential financial gain, or strategic importance.
Collaboration [42]	Cybercriminals often collaborate and share information, tools, and resources with other threat actors, allowing them to pool resources and knowledge to launch more effective attacks.
Motivations [25][40]	Cyber threats to the financial sector are often financially motivated, with attackers seeking to steal funds, commit fraud, or demand ransom. However, other motivations can include espionage, disruption, or political objectives, especially in the case of nation-state actors.

D. CRITERIA USED TO CLASSIFY CYBER THREATS.

In this section we will explore in depth to explore criteria used to classify cyber threats with some examples for each criterion. The specific characteristics of the threat, which in turn can help in determining the most appropriate response strategies. Understanding the various criteria used to classify cyber threats is vital for developing effective countermeasures. By analyzing the threat vector, attack surface, attack type, threat severity, threat origin, threat impact, attack objective, frequency, attack complexity, and threat actor can gain a better understanding of the cyber threat landscape and tailor their response strategies accordingly. By employing these criteria, we aim to create a comprehensive and well-rounded classification framework that captures the diverse dimensions of cyber threats. Each criterion is accompanied by a detailed description that clarifies its significance and applicability within the classification process. In TABLE 4, we classify various criteria of cyber threats into different dimensions.

The awareness of the examples provided for each criterion helps to develop a comprehensive understanding of the various threat scenarios. This knowledge will allow organizations to prioritize cybersecurity investments, implement appropriate security controls, and continuously monitor and adjust the defenses in response to the ever-evolving cyber threat landscape. Ultimately, a comprehensive understanding of these criteria and examples will enable to maintain the security, confidentiality, and integrity of their systems and data, protecting both their organizations and their customers from the detrimental effects of cyber threats. Establishing a set of criteria for classifying cyber threats is paramount in developing a comprehensive understanding of the threat landscape. In this section, we delve into an in-depth analysis of the criteria employed to classify cyber threats, enabling a systematic and structured approach to threat categorization. We have identified and defined the key criteria used to classify these threats, providing a framework that enhances the ability to assess, prioritize, and respond to cyber risks effectively. Through this process, we have established a set of criteria that guide the classification of cyber threats. These criteria encompass technical factors, such as the nature of the attack, the vulnerability exploited, and the level of sophistication exhibited. Additionally, non-technical factors, such as the motives of threat actors, the scope of impact, and the potential for financial loss or reputational damage, are considered. Employing these criteria aims to create a comprehensive and well-rounded classification framework that captures the diverse dimensions of cyber threats. Each criterion is accompanied by a detailed description that clarifies its significance and applicability within the classification process. In TABLE 4, we classify various criteria of cyber threats into different dimensions.

The classification criteria for cyber threats are shown in Table 4 ranked based on severity, their importance and potential impact. Threat Impact is ranked as the most important criterion because it measures the potential damage that a cyber threat can cause to banking and financial services. Threat Severity is ranked second because it measures the seriousness of a cyber threat in terms of its potential impact. Attack Type is ranked third because it measures the method used by cybercriminals to launch an attack. Threat Vector is ranked fourth because it measures the path used by cybercriminals to reach their target. Threat Origin is ranked fifth because it measures the source of the cyber threat. Threat Actor and Threat Motivation are ranked sixth and seventh because they measure the identity and motive of the cybercriminals behind the attack. Vulnerability Type and Targeted Assets are ranked eighth and ninth because they measure the specific weaknesses and assets that are targeted by cybercriminals. Detection and Response Capabilities are ranked tenth because they measure the ability of banking and financial services to detect and respond to cyber threats. Attack Complexity, Attack Surface, and Attack Objective are ranked eleventh to thirteenth because they measure the level of difficulty, scope, and goal of the cyber-attack. Countermeasure Effectiveness is ranked fourteenth because it measures the effectiveness of the countermeasures used to prevent or mitigate cyber threats.

TABLE 4. Dimensions of cyber threats criteria.

Dimension	Description	Criteria under dimension
Threat Characteristics Dimension	This dimension captures the nature of the threat itself	Attack Type [44], Threat Vector [41], Threat Origin [42], Vulnerability Type [38], Attack Complexity [32][44], Attack Surface [32], Threat Lifecycle [45], Tools and Techniques [16][41], Frequency [41]
Threat Actor Dimension	This dimension focuses on the entity or entities responsible for the threat	Threat Actor [43], Threat Motivation [43], Geographical Distribution [42]
Impact Dimension	This dimension assesses the potential or actual consequences of a threat	Threat Impact [33][44], Threat Severity [33], Targeted Assets [43], Attack Objective [30]
Defense Dimension	This dimension concerns the capabilities and actions of the target to detect, respond, and prevent threats	Detection and Response Capabilities [31], Countermeasure Effectiveness [30], Indicators of Compromise (IoCs) [46]
Future Trends Dimension	This dimension anticipates the evolution of cyber threats	Emerging Trends and Technologies [47]

Threat Lifecycle is ranked fifteenth because it measures the different stages of a cyber threat, from reconnaissance to exploitation to exfiltration. Indicators of Compromise (IoCs) and Tools and Techniques are ranked sixteenth and seventeenth because they measure the specific indicators and tools used by cybercriminals to launch an attack. Frequency is ranked eighteenth because it measures the frequency of cyber threats. Geographical Distribution is ranked nineteenth because it measures the geographic scope of cyber threats. Emerging Trends and Technologies are ranked twentieth because they measure the potential impact of new and emerging technologies on cyber threats.

E. TREATS CLASSIFICATION

In this section, we present a comprehensive classification of threats in the context of the Banking and Financial Sector. The classification framework is organized into two main categories: technical threats and non-technical threats. Each category is further subdivided into specific threat types, providing a detailed taxonomy that facilitates a systematic and holistic understanding of the threat landscape. By classifying threats, we aim to enhance the effectiveness of threat analysis, incident response, and risk management strategies. In this section, we present a table summarizing the threat categories, their descriptions, and relevant examples, shedding light on the diverse range of threats that the Banking and Financial Sector faces. Effective classification of cyber threats is essential for understanding and mitigating risks in the ever-evolving landscape of cybersecurity. In this section, we present a systematic and comprehensive approach to classifying threats in the context of the Banking and Financial Sector. The classification process entails a meticulous analysis of various threat dimensions, allowing for a nuanced understanding of the diverse range of threats faced by the sector.

The classification framework is structured into two main categories: technical threats and non-technical threats. Technical threats encompass malicious activities that exploit vulnerabilities in technological systems, such as network breaches, malware attacks, and distributed denial-of-service (DDoS) attacks. Non-technical threats, on the other hand, include social engineering tactics, insider threats, and regulatory non-compliance, which focus on human factors, policy violations, and legal aspects. Within each category, threat types are further delineated to capture specific manifestations of threats. For example, under technical threats, subcategories may include network-based threats, application-based threats, and infrastructure-based threats. Similarly, non-technical threats can be categorized into social engineering attacks, physical security breaches, and legal and compliance violations. The classification process draws upon a multidimensional analysis of threat characteristics, impact factors, and attack vectors. Each threat category is accompanied by a description that elucidates its nature and potential implications for the Banking and Financial Sector. Additionally, relevant examples and detailed descriptions of notable incidents or attack scenarios are provided to enhance understanding and contextualize the threats within the sector. In the subsequent sections, we present the detailed classification framework,

TABLE 5. Classification criteria for CYBER threats.

Criteria	Description	Examples
Threat Impact [33][44]	The consequences of a successful cyber-attack, which can include financial, operational, reputational, or legal ramifications.	a. Financial consequences b. Operational consequences c. Reputational consequences d. Legal consequences e. Regulatory penalties f. Loss of customer trust g. Competitive disadvantages h. Increased costs of mitigation and recovery i. Disruption of critical services j. Data loss or destruction
Threat Severity [33]	The level of potential harm or damage that could be caused by a cyber threat if successfully executed.	a. High-severity threats b. Medium-severity threats c. Low-severity threats d. Data breaches e. Intellectual property theft f. Business email compromise (BEC) g. Payment fraud h. System outages i. Account takeover j. Identity theft
Attack Type [44]	The specific technique or method employed by a cyber attacker to exploit a vulnerability and gain unauthorized access.	a. SQL injection b. Cross-site scripting (XSS) c. Brute-force attacks d. Man-in-the-middle (MitM) attacks e. Password spraying f. Zero-day exploits g. Privilege escalation h. Remote code execution i. Drive-by downloads j. DNS poisoning.
Threat Vector [41]	The method or pathway used by a cyber attacker to gain unauthorized access to a target system or network.	a. Phishing b. Spear-phishing c. Whaling d. Clone phishing e. Malware f. Ransomware g. social engineering h. Denial-of-service (DoS) attacks i. Distributed denial-of-service (DDoS) attacks j. Insider threats.
Threat Origin [42]	The source or entity responsible for initiating a cyber threat, which could be internal, external, or a combination of both.	a. Internal threats b. External threats c. State-sponsored attacks d. Cybercriminals e. Hacktivists f. Insider threats g. Rogue employees h. Third-party vendors i. Supply chain attacks j. Cyber mercenaries
Threat Actor[43]	The individual or group responsible for initiating a cyber threat.	a. Hacktivists b. Cybercriminals c. State-sponsored groups d. Insiders e. Rogue employees f. Third-party vendors g. Cyber mercenaries h. Organized crime syndicates i. Terrorist organizations j. Cyber espionage groups
Threat Motivation [43]	The underlying reasons driving a cyber attacker.	a. Financial motives b. Political motives c. Ideological motives d. Personal motives e. Competition-driven motives f. Revenge motives g. Nation-state interests h. Cyber warfare i. Market advantage j. Intellectual property theft
Vulnerability Type [38]	The specific weakness or flaw in a system, application, or process that can be exploited by a cyber attacker.	a. Software vulnerabilities b. Hardware vulnerabilities c. Configuration vulnerabilities d. Communication vulnerabilities e. Human vulnerabilities (social engineering) f. Third-party/vendor vulnerabilities g. Cryptographic vulnerabilities h. Zero-day vulnerabilities i. Known vulnerabilities j. Unpatched vulnerabilities
Targeted Assets [43]	The specific data, systems, or infrastructure that a cyber attacker aims to compromise or gain access to.	a. Customer data b. Employee data c. Financial data d. Intellectual property e. Trade secrets f. Banking infrastructure g. Payment systems h. Online banking platforms i. Mobile banking apps j. ATM networks
Detection and Response Capabilities [31]	The ability to identify, monitor, and respond to cyber threats, using tools.	a. Proactive detection b. Reactive detection c. Incident response capabilities d. Threat intelligence e. Security automation f. Threat hunting g. Forensic investigation h. Security orchestration, automation, and response (SOAR) i. Endpoint detection and response (EDR) j. Security information and event management (SIEM) systems
Attack Complexity [32][44]	The level of difficulty and sophistication involved in executing a cyber-attack, including the use of advanced techniques or tools.	a. Simple attacks b. Complex attacks c. Multi-vector attacks d. Fileless malware attacks e. Advanced evasion techniques f. Social engineering attacks g. Customized malware h. Encrypted attacks i. Living-off-the-land attacks j. Machine learning-based attacks
Attack Surface [32]	The sum of all potential points of vulnerability within a system or network that can be exploited by a cyber attacker.	a. Web applications b. Static web applications c. Dynamic web applications d. Mobile web applications e. Network devices f. Routers g. Switches h. Firewalls i. Databases j. Endpoints.
Attack Objective [30]	The goal or intent of a cyber attacker.	a. Financial gain b. Data theft c. Espionage d. Sabotage e. Hacktivism f. Political objectives g. Industrial espionage h. Market manipulation i. Competitor disruption j. Reputation damage
Countermeasure Effectiveness [30]	The success or efficacy of security measures implemented to prevent, detect, or mitigate the impact of cyber threats.	a. Preventive measures b. Detective measures c. Corrective measures d. Deterrent measures e. Recovery measures f. Adaptive measures g. Security awareness training h. Patch management i. Access control j. Intrusion prevention systems (IPS)
Threat Lifecycle [45]	The stages a cyber-attack progresses through, from initial compromise to exploitation, lateral movement, and eventual data exfiltration or system damage.	a. Initial compromise b. Exploitation c. Lateral movement d. Command and control e. Data exfiltration f. Persistence g. Privilege escalation h. Reconnaissance i. Weaponization j. Delivery
Indicators of Compromise (IoCs) [46]	Observable data points that suggest a system or network has been breached or compromised by a cyber attacker.	a. IP addresses b. Domain names c. URLs d. File hashes e. Email addresses f. Registry keys g. Malware signatures h. Network traffic patterns i. System behaviors j. Log anomalies
Tools and Techniques [16][41]	The specific software, hardware, or methods employed by cyber attackers to carry out their activities.	a. Exploit kits b. Command and control servers c. Botnets d. Ransomware-as-a-Service (RaaS) e. Cryptocurrency mining malware f. Advanced Persistent Threat (APT) toolkits g. Keyloggers h. Remote Access

TABLE 5. *(Continued.)* **Classification criteria for CYBER threats.**

		Trojans (RATs) i. Password stealers j. Fileless malware
Frequency [41]	The rate at which cyber-attacks occur, ranging from one-time incidents to recurring or persistent threats.	a. One-time attacks b. Recurring attacks c. Advanced persistent threats (APTs) d. Targeted attacks e. Opportunistic attacks f. Seasonal attacks (e.g., during tax season or holidays) g. Coordinated attacks h. Campaign-based attacks i. Continuous scanning and probing j. Multi-stage attacks
Geographical Distribution [42]	The location or region where cyber-attacks originate, as well as the distribution of victims across different countries or areas.	a. Origin of the attack b. Geographical distribution of the victims c. Jurisdictional challenges d. Cross-border collaboration e. Regional threat actors f. Geopolitical considerations g. Safe havens for cybercriminals h. Countery Cybersecurity laws and regulations i. International cooperation j. Attack patterns and trends
Emerging Trends and Technologies [47]	New developments and advancements in technology that can present both opportunities and challenges for cybersecurity efforts.	a. Artificial intelligence (AI) and machine learning (ML) in cyber-attacks b. Internet of Things (IoT) security c. Cloud security d. Quantum computing and cryptography e. 5G network security f. Blockchain and distributed ledger technology (DLT) security g. Cyber-physical systems security h. Privacy-enhancing technologies i. Augmented and virtual reality (AR/VR) security j. Biometric security.

including the taxonomy of technical and non-technical threats TABLE 7 and TABLE 9 respectively, along with comprehensive descriptions and examples for each threat category.

1) TECHNICAL THREATS

Technical threats are those threats that involve the use of technology, tools, or techniques to exploit vulnerabilities in a system, network, or application. The technical threats are classified into distinct dimensions based on their characteristics and areas of impact as mentioned in TABLE 6.

TABLE 7 presents a prioritized list of technical threats, arranged according to their severity and potential impact on the banking and financial services sector. Advanced Persistent Threats (APT) is considered the most severe and impactful threat as it involves a sophisticated, long-term attack on a specific target, such as a financial institution, with the goal of stealing sensitive information. Phishing and malware are also considered serious threats as they can lead to unauthorized access to sensitive information and financial transactions. Distributed Denial of Service (DDoS) attacks, supply chain attacks, web application attacks, mobile banking threats, and cloud security threats are other technical threats that can impact banking and financial services. Internet of Things (IoT) threats, account takeover threats, cryptojacking, zero-day exploits, man-in-the-middle attacks, password attacks, credential stuffing, deepfakes and disinformation, zero-day vulnerabilities, quantum computing threats, and third-party and vendor risks are also potential threats to banking and financial services.

TABLE 6. **Dimensions of technical threats.**

Dimension	Description	Example of technical threats
Persistent and Sophisticated Threats Dimension	This dimension focuses on advanced, persistent threats that typically require significant resources and expertise to execute and mitigate.	Advanced Persistent Threats [86] Zero-day Exploits [50] Zero-day Vulnerabilities [50]
Software and Web Application Threats Dimension	Threats in this dimension exploit vulnerabilities in software, web applications, and services.	Malware [33] Web Application Attacks [26][44] Supply Chain Attacks [53] Third-party and vendor risks [53] Zero-day Vulnerabilities [50]
Social Engineering and Deceptive Threats Dimension	This dimension encompasses threats that rely on manipulation and deceit, often involving the impersonation of legitimate entities or processes	Phishing [30] Deepfakes and Disinformation [51] Account Takeover Threats [87]
Disruptive Threats Dimension	Threats within this dimension are designed to interrupt services and infrastructure, often causing significant operational impact	Distributed Denial of Service [30] Cryptojacking [50]
Credential and Access Threats Dimension	This dimension relates to threats that involve unauthorized access to systems, often via stolen or compromised credentials	Password Attacks [89] Credential Stuffing [90] Account Takeover Threats [87]
Emerging Technology Threats Dimension	This dimension captures threats related to new and rapidly evolving technologies	Mobile Banking Threats [48] Cloud Security Threats [49] Internet of Things (IoT) Threats [26][44] Quantum Computing Threats [52] Cryptocurrency-related Threats [50]
Network-based Threats Dimension	This dimension includes threats that exploit vulnerabilities in network communications and protocols	Man-in-the-middle Attacks [88]

2) NON-TECHNICAL THREATS

Non-technical threats are those that involve manipulating human behavior or exploiting human vulnerabilities to gain unauthorized access to sensitive information or systems. It poses significant challenges and can often be more difficult to mitigate due to their reliance on human factors, organizational policies, and legal complexities. These threats are

TABLE 7. Technical threats.

Category	Description	Examples	Examples Description
Advanced Persistent Threats [86]	Sophisticated, often state-sponsored, cyberattacks that persist undetected for an extended period of time.	Multi-stage attacks	Use a combination of social engineering, malware, and network exploitation to infiltrate a system and remain undetected.
		Targeted data exfiltration	Focus on stealing specific sensitive information from the target organization.
Malware [33]	Malicious software designed to compromise, damage, or gain unauthorized access to computer systems or networks.	Banking Trojans	Steal banking credentials by intercepting login information and redirecting users to fake banking websites.
		Ransomware	Encrypt files on a system and demand payment in exchange for the decryption key.
Phishing [30]	Deceptive emails or messages attempting to trick users into revealing sensitive information or installing malware.	Spear-phishing	Highly targeted phishing attacks aimed at specific individuals or organizations.
		Clone phishing	Attackers replicate a legitimate email and modify the content or links to deceive the recipient.
Distributed Denial of Service [30]	Overwhelming a target system or network with traffic, rendering it inaccessible or unusable.	Application-layer attacks	Target specific applications and exhaust server resources.
		Protocol-based attacks	Exploit weaknesses in network protocols to overwhelm the 5target system.
Supply Chain Attacks [53]	Cyberattacks targeting vulnerabilities in a company's supply chain or third-party vendors.	Software compromise	Attackers infiltrate a software vendor's infrastructure to insert malicious code into legitimate software updates.
		Hardware compromise	Manipulate hardware components or devices to compromise a target organization's systems.
Web Application Attacks [26][44]	Cyberattacks targeting vulnerabilities in web applications, such as SQL injection or cross-site scripting.	Cross-site request forgery (CSRF)	An attacker tricks a victim into performing actions on their behalf, such as transferring funds or changing account settings.
		Insecure direct object references (IDOR)	Attackers exploit improper access controls to access unauthorized resources, like another user's account information.
Mobile Banking Threats [48]	Cybersecurity risks and vulnerabilities specifically targeting mobile banking apps and platforms.	Fake banking apps	Cybercriminals create counterfeit apps that mimic legitimate banking apps to trick users into revealing their login credentials.
		Mobile malware	Attackers use malware to target mobile devices, stealing sensitive information, intercepting communications, or compromising mobile banking apps.
Cloud Security Threats [49]	Cybersecurity challenges and risks associated with the use and management of cloud-based services and infrastructure.	Misconfigurations	Insecure configurations in cloud environments can expose sensitive data or enable unauthorized access to systems.
		Data breaches	Attackers can exploit vulnerabilities in cloud services to gain access to sensitive information stored in the cloud.
Internet of Things (IoT) Threats [26][44]	Security vulnerabilities and risks related to connected devices, often lacking robust security measures.	Insecure devices	IoT devices with weak security features or vulnerabilities can be exploited by attackers to gain access to networks and sensitive information.
		Botnets [30]	Compromised IoT devices can be used to launch large-scale DDoS attacks or distribute malware.
Account Takeover Threats [87]	Unauthorized access to and control of a user's online accounts, often for financial gain or identity theft.	Credential stuffing	Use stolen login credentials from previous data breaches to gain unauthorized access to accounts.
		Password spraying	Attempt to gain access to accounts using common passwords and multiple username combinations.
Cryptojacking [50]	The unauthorized use of a victim's computing resources for mining cryptocurrency.	In-browser cryptojacking	Attackers exploit vulnerabilities in web applications to run cryptocurrency mining scripts on users' browsers without their consent.
		System-based cryptojacking	Malware infects a target system and secretly mines cryptocurrency using the system's resources.
Zero-day Exploits [50]	Cyberattacks that exploit previously unknown vulnerabilities before they can be patched or fixed.	Exploiting unknown vulnerabilities	Attackers use previously undisclosed security vulnerabilities to compromise systems before vendors can issue patches or updates.
		Targeted attacks	Cybercriminals often use zero-day exploits to target high-value organizations, like banks and financial institutions.
Man-in-the-middle Attacks [88]	Unauthorized interception and manipulation of communication between two parties.	Session hijacking	Attackers intercept and take control of a user's session, potentially gaining access to sensitive information or performing unauthorized actions.
		SSL/TLS interception	Compromise the secure communication between a user and a web service by intercepting and decrypting encrypted data.
Password Attacks [89]	Various techniques for cracking or guessing user passwords, such as brute-force or dictionary attacks.	Brute-force attacks	Attempt to gain access to an account by systematically trying all possible password combinations.
		Dictionary attacks	Use a list of common or previously exposed passwords to gain access to accounts.
	Automated attempts to	Automated attacks	Attackers use automated tools to try previously

TABLE 7. *(Continued.)* **Technical threats.**

Credential Stuffing [90]	gain unauthorized access to accounts using stolen or leaked credentials.	Account takeover	leaked username and password combinations on various online services, hoping to find a match. Once attackers gain access to an account, they can steal sensitive information, transfer funds, or commit fraud.
Deepfakes and Disinformation [51]	The use of AI-generated audio, video, or text content to spread false or misleading information.	Fraud	Deepfake technology can be used to create convincing fake audio or video content to deceive victims, impersonate executives, or manipulate stock prices.
		Reputation damage	Disinformation campaigns can target banks or financial institutions, spreading false information to undermine trust or cause reputational harm.
Zero-day Vulnerabilities [50]	Undiscovered security flaws in software or hardware that can be exploited by cyber attackers.	Exploit development	Attackers can discover and exploit unknown vulnerabilities in software or hardware, allowing them to bypass security measures and infiltrate systems.
		Advanced targeted attacks	Cybercriminals may use zero-day exploits to carry out sophisticated, targeted attacks on banks and financial institutions.
Quantum Computing Threats [52]	Emerging cybersecurity challenges posed by advances in quantum computing and their potential impact on encryption.	Encryption breaking	As quantum computing becomes more advanced, it could potentially be used to break existing encryption algorithms, undermining data security.
Third-party and vendor risks [53]	Cyber risks associated with reliance on third-party vendors or service providers with their own security vulnerabilities.	Data breaches	Vendors or third-party service providers with access to sensitive information may experience a data breach, potentially exposing bank or customer data.
		Supply chain compromise	Attackers can target third-party vendors or service providers to gain access to a bank's systems or data indirectly.
Cryptocurrency-related Threats [50]	Cyber threats targeting the theft or manipulation of digital currencies, wallets, or exchanges.	Cryptojacking	Attackers use malware to hijack victims' computing resources to mine cryptocurrencies without their knowledge or consent.
		Fraudulent Initial Coin Offerings (ICOs)	Cybercriminals may create fake ICOs to defraud investors or use ICO platforms to conduct phishing attacks.

categorized into several distinct dimensions based on their sources and nature.

Table 9 ranks the non-technical threat based on the frequency and potential impact on banking and financial services. Insider threats and social engineering are considered the most severe non-technical threats for banking and financial services. Identity theft and business email compromise are also serious threats that can result in significant financial losses. Physical security breaches and third-party risk are other non-technical threats that pose a risk to banking and financial services. Employee negligence and lack of awareness, human error, legal and regulatory risks, shadow IT, and social media threats are less severe but still pose a potential risk to banking and financial services.

TABLE 8. **Dimensions of non-technical threats.**

Dimension	Description	Example of technical threats
Internal Threats Dimension	This dimension focuses on threats that originate from within the organization and often involve trusted insiders	Insider Threats [30] Employee negligence and lack of awareness [57] Human error [58] Shadow IT [59]
Social Engineering and Identity Fraud Dimension	Threats in this dimension exploit human tendencies to trust and deceive, often with the goal of stealing personal information or manipulating individuals into granting access to secure systems	Social Engineering [50] Identity Theft [54] Business Email Compromise (BEC) [55] Social media threats [60]
Physical Security Breaches Dimension	This dimension encompasses threats that involve physical access or manipulation of hardware, facilities, or people.	Physical security breaches [56]
Third-party Risks Dimension	This dimension relates to threats that stem from external entities with whom the organization has a business relationship	Third-party risk [53]
Legal and Regulatory Risks Dimension	Threats in this dimension involve the potential for non-compliance with applicable laws, regulations, or standards, which can result in penalties or other negative consequences	Legal and regulatory risks [61]

V. COUNTERMEASURES

Developing effective countermeasures is crucial in mitigating the risks posed by cyber threats within the Banking and Financial Sector. In this section, we delve into an extensive analysis of countermeasures aimed at mitigating the impact and reducing the vulnerabilities associated with cyber threats. By following a rigorous process, we have examined and categorized a range of countermeasures, providing a comprehensive framework to enhance the sector's resilience against cyber-attacks. The development of countermeasures involved a systematic and multifaceted approach. We conducted an in-depth review of industry best practices, academic studies,

TABLE 9. Non-technical threats.

Non-technical Threats	Type	Description
Insider Threats [30]	a. Intentional insider threats	Individuals with authorized access to a system act with malicious intent to cause harm.
	b. Unintentional insider threats	Employees or contractors inadvertently cause security breaches due to negligence or lack of awareness.
Social Engineering[50]	a. Pretexting	Attackers create a fabricated scenario to manipulate the victim into providing sensitive information or access.
	b. Baiting	Lure victims with promises of free items or services to encourage them to click on malicious links or download malware.
Identity Theft [54]	a. Financial identity theft	Steal personal information to fraudulently access funds or open new accounts in the victim's name.
	b. Medical identity theft	Obtain medical services or medications using the victim's personal information.
Business Email Compromise (BEC) [55]	a. CEO fraud	Attackers impersonate a high-level executive and send fraudulent emails to employees, instructing them to transfer funds or reveal sensitive information.
	b. Invoice fraud	Attackers pose as a legitimate vendor or supplier and request payment for fraudulent invoices.
Physical security breaches [56]	a. Unauthorized access	Attackers gain physical access to a facility or data center to compromise systems or steal sensitive information.
	b. Hardware tampering	Modify or replace hardware components to introduce vulnerabilities or compromise the target system.
Third-party risk [53]	a. Vendor risk	Attackers exploit vulnerabilities in third-party vendors' systems to gain access to a target organization's sensitive information or systems.
	b. Service provider risk	Inadequate security measures by service providers can expose customer data.
Employee negligence and lack of awareness [57]	a. Poor password management	Employees use weak passwords or reuse passwords across multiple accounts, increasing the risk of account compromise.
	b. Inadequate security training	Employees lack the necessary knowledge to recognize and respond to potential security threats.
Human error [58]	a. Accidental data exposure	Employees inadvertently disclose sensitive information through email, file-sharing platforms, or other communication channels.
	b. Misconfiguration	Employees unintentionally leave systems or data exposed due to incorrect configurations or a lack of understanding of security best practices.
Legal and regulatory risks [61]	a. Non-compliance	Failing to comply with data protection regulations or industry-specific standards can result in fines and reputational damage.
	b. Data privacy breaches	Unauthorized access to or disclosure of personal information can lead to legal liabilities and reputational harm.
Shadow IT [59]	a. Unauthorized software and services	Employees use unapproved software or services without the knowledge or approval of IT, creating potential security risks.
	b. Data leakage	The use of unauthorized tools or services can lead to the exposure of sensitive data.
Social media threats [60]	a. Information leakage	Employees may inadvertently share sensitive information on social media platforms, which can be exploited by attackers.
	b. Social engineering	Attackers can use social media to gather information about employees or the organization, facilitating targeted attacks.

cybersecurity frameworks, and expert recommendations to identify and analyze a diverse range of countermeasures.

We focused on strategies and techniques that address specific threat categories, enhance security postures, and fortify critical infrastructure within the Banking and Financial Sector. Through this process, we have categorized countermeasures into distinct dimensions. These dimensions include technical measures, such as network segmentation, encryption, intrusion detection systems, and vulnerability patching. Additionally, non-technical measures, which consists of Organizational, Legal and Regulatory Measures such as employee training, incident response planning, threat intelligence sharing, and regulatory compliance, are considered. By organizing countermeasures into these dimensions, we aim to provide a comprehensive understanding of the diverse range of strategies that can be employed to mitigate cyber risks. Each dimension is accompanied by a detailed description, highlighting its significance and potential impact within the sector. This approach not only enhances our knowledge of effective defense mechanisms but also equips stakeholders with actionable insights to develop tailored cybersecurity strategies and safeguard their operations, data, and reputation. Figure 3 shows the cyber threats countermeasures.

A. TECHNICAL CONTROLS

Technical countermeasures are tools and techniques designed to protect systems and data from cyber threats. They

are essential for safeguarding the integrity of information systems, networks, and data from unauthorized access and cyberattacks. They can be classified into several dimensions based on their primary functions and use cases. Table 10 shows the dimensions of the technical controls.

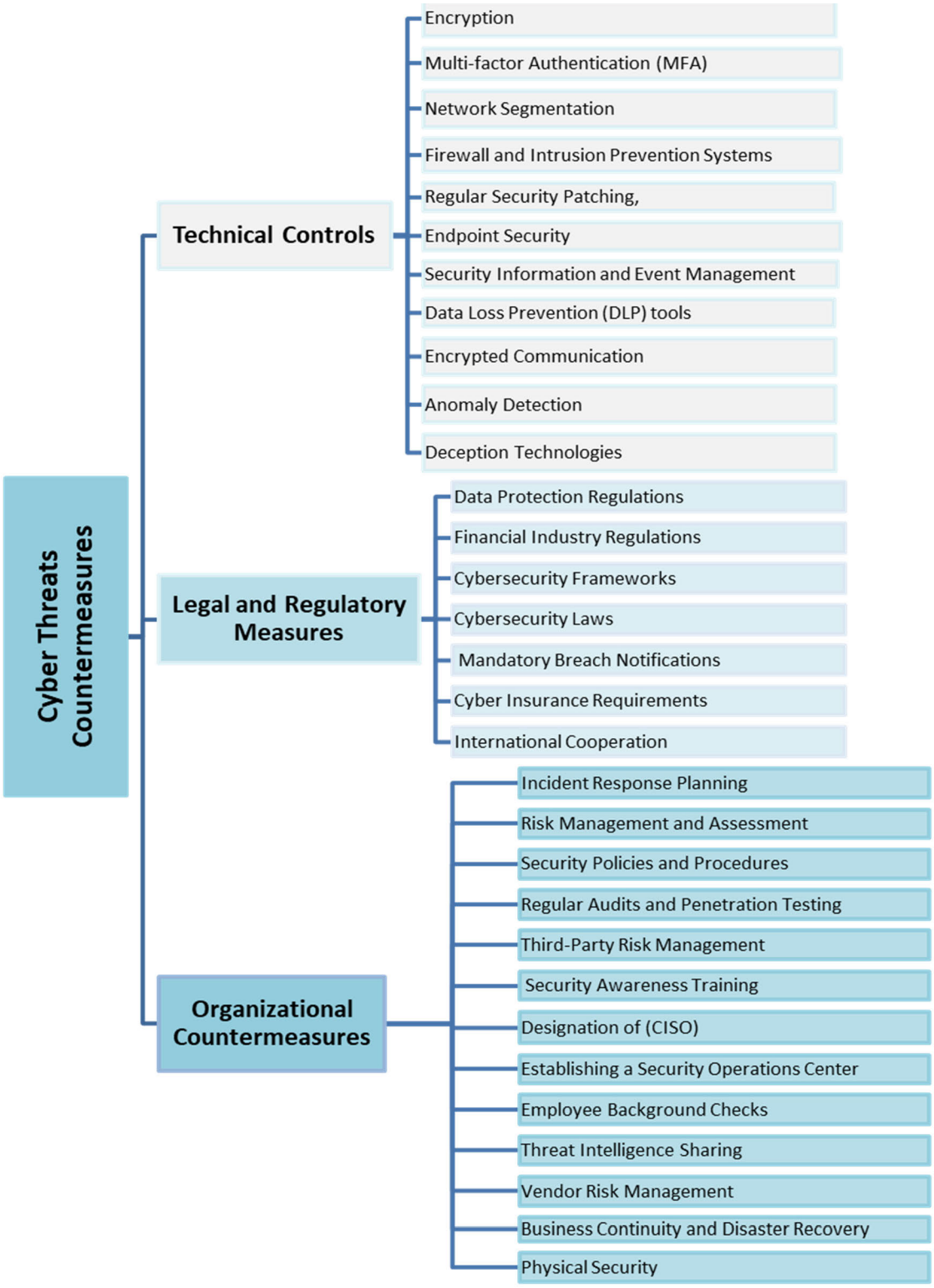

FIGURE 3. Cyber threats countermeasures.

Table 11 shows the ranking of the Technical Controls for banking and financial services based on their effectiveness and importance. Encryption is considered the most effective and important technical control for banking and financial services as it helps to protect sensitive data and prevent unauthorized access. Multi-factor authentication (MFA) and network segmentation are also highly effective in preventing unauthorized access to systems and data. Firewall and Intrusion Prevention Systems (IPS), regular security patching, endpoint security, and Security Information and Event Management (SIEM) are also important technical controls for banking and financial services. Data Loss Prevention (DLP) tools, encrypted communication, anomaly detection, and deception technologies are also important technical controls that can help to prevent and detect cyberattacks. Overall, the effectiveness and importance of these technical controls may vary depending on the specific needs and risks of each organization. Therefore, it is essential for banking and financial services to assess their cybersecurity risks and implement a comprehensive cybersecurity strategy that includes a combination of technical controls, policies, and procedures to mitigate the risks.

TABLE 10. Dimensions of technical controls.

Dimension	Description	Example of technical threats
Authentication and Access Control Dimension	This dimension includes technologies that verify the identities of users and control their access to systems and data	• Multi-factor Authentication (MFA) [62] • Encrypted Communication [70]
Network Security Dimension	Countermeasures in this dimension focus on protecting the integrity and functionality of the network	• Network Segmentation [66] • Firewall and Intrusion Prevention Systems (IPS) [30]
Data Protection Dimension	This dimension includes countermeasures that primarily focus on protecting data from unauthorized access or loss	• Encryption • Regular Security Patching [63] • Data Loss Prevention (DLP) tools [67]
Endpoint Security Dimension	This dimension focuses on securing endpoints in the network to prevent unauthorized access and protect against threats	• Endpoint Security [65]
Security Monitoring and Response Dimension	Countermeasures in this dimension help to identify, analyze, and respond to security events and incidents	• Security Information and Event Management (SIEM) [64] • Anomaly Detection [68] • Deception Technologies [69]

TABLE 11. Technical controls.

Technical Countermeasures	Description
Encryption [70]	Banks use encryption to protect sensitive data, both in transit and at rest. Encryption ensures that data can only be accessed and read by authorized individuals, preventing unauthorized access and data breaches.
Multi-factor Authentication (MFA) [62]	MFA requires users to provide multiple forms of identification before accessing sensitive systems or data. This can include passwords, biometrics, or hardware tokens, making it more difficult for attackers to gain unauthorized access using stolen credentials.
Network Segmentation [66]	Network segmentation involves separating different parts of the network to limit unauthorized access and the potential spread of an attack.
Firewall and Intrusion Prevention Systems (IPS) [30]	Firewalls and IPS protect the internal network of banks from unauthorized access and intrusion attempts. They monitor incoming and outgoing network traffic, blocking malicious activity, and preventing unauthorized access to sensitive data.
Regular Security Patching [63]	Banks must keep their systems and software up-to-date by applying security patches and updates regularly. This helps to close known vulnerabilities that attackers could exploit.
Endpoint Security [65]	Implementing endpoint security solutions, such as antivirus and antimalware software, helps protect individual devices from threats like malware, ransomware, and targeted attacks.
Security Information and Event Management (SIEM) [64]	SIEM systems collect, analyze, and correlate data from various sources to detect and respond to potential security incidents. They provide real-time monitoring and alerts, enabling banks to respond quickly to cyber threats.
Data Loss Prevention (DLP) tools [67]	DLP tools monitor and prevent the unauthorized transmission of sensitive data, both within and outside the organization.
Encrypted Communication [70]	Using encrypted communication channels, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), protects sensitive data in transit and prevents unauthorized access or interception.
Anomaly Detection [68]	Implementing machine learning-based anomaly detection systems helps identify unusual patterns in network traffic, user behavior, or transactions, which may indicate potential threats.
Deception Technologies [69]	Deception technologies create decoy systems, such as honeypots, that lure attackers and enable organizations to study their tactics, techniques, and procedures (TTPs) without risking real systems or data.

B. LEGAL AND REGULATORY MEASURES

Legal and regulatory measures play an integral role in shaping the cybersecurity landscape. They are designed to enforce compliance with established rules, guidelines, and standards that govern data protection, privacy, and cybersecurity within the banking and financial sectors. These measures can be categorized into several dimensions as illustrated in Table 12, each focusing on a specific aspect of legal and regulatory cybersecurity controls.

TABLE 12. Dimensions of legal and regulatory measures.

Dimension	Description	Example of technical threats
Data Protection Dimension	This dimension includes measures focused on the protection of personal and sensitive data.	• Data Protection Regulations [71]
Financial Industry Regulations Dimension	This dimension encompasses regulations specifically designed for the financial sector	• Financial Industry Regulations [72]
Frameworks and Best Practices Dimension	This dimension covers measures that provide structured approaches and guidelines for cybersecurity	• Cybersecurity Frameworks [73]
Legal Sanctions and Obligations Dimension	This dimension includes laws and requirements that impose legal obligations on entities to maintain a certain level of cybersecurity	• Cybersecurity Laws [74] • Mandatory Breach Notifications [74][75] • Cyber Insurance Requirements [76]
International Cooperation Dimension	This dimension covers measures that involve collaboration and agreement among different countries or international entities	• International Cooperation [77]

Table 13 shows the ranking of the legal and regulatory measures for banking and financial services based on their effectiveness and importance. Data Protection Regulations and Financial industry regulations are considered the most effective and important legal and regulatory measures for banking and financial services as they provide clear guidelines and standards for cybersecurity. Cybersecurity frameworks and laws are also important legal and regulatory measures that can help to establish cybersecurity standards and requirements for the industry. Data protection regulations and mandatory breach notifications are also important legal and regulatory measures that can help to protect sensitive data and ensure timely reporting of cybersecurity incidents. Cyber insurance requirements and international cooperation are also important legal and regulatory measures that can help to mitigate the financial and reputational risks associated with cybersecurity incidents. Overall, the effectiveness and importance of these legal and regulatory measures may vary depending on the specific needs and risks of each organization. Therefore, it is essential for banking and financial services to comply with the relevant regulations and standards, and to implement a comprehensive cybersecurity strategy that includes a combination of legal and regulatory measures, technical controls, policies, and procedures to mitigate the risks.

C. ORGANIZATIONAL COUNTERMEASURES

Organizational countermeasures focus on fostering a security-conscious culture within the financial institution.

TABLE 13. Legal and regulatory measures.

Legal and Regulatory Measures	Description
Data Protection Regulations [71]	Banks must comply with data protection regulations, such as the General Data Protection Regulation (GDPR)[93] in the EU, the California Consumer Privacy Act (CCPA)[96] in the US, and similar laws in other jurisdictions. These regulations impose strict requirements on how banks collect, process, and store personal data, ensuring that sensitive information is protected from unauthorized access and misuse.
Financial Industry Regulations [72]	Banks must also comply with financial industry-specific regulations, such as the Payment Card Industry Data Security Standard (PCI-DSS)[94], which sets security standards for handling cardholder data, and the Bank Secrecy Act (BSA)[95], which requires banks to report suspicious activities to authorities.
Cybersecurity Frameworks [73]	Various cybersecurity frameworks, such as the NIST Cybersecurity Framework and the ISO/IEC 27001 standard, provide guidelines and best practices for banks to implement robust cybersecurity measures.
Cybersecurity Laws [74]	National and international cybersecurity laws impose penalties and fines on banks that fail to implement adequate security measures or report security incidents in a timely manner.
Mandatory Breach Notifications [74][75]	Laws in many jurisdictions require banks to notify customers and authorities in the event of a data breach, ensuring transparency and encouraging proactive cybersecurity measures.
Cyber Insurance Requirements [76]	Regulators may require banks to hold cyber insurance policies, which help cover financial losses resulting from cyber-attacks and can incentivize organizations to maintain robust security practices.
International Cooperation [77]	Governments and financial regulators should collaborate on a global scale to share threat intelligence, best practices, and legal frameworks to combat cyber threats effectively.

This involves regular employee training and awareness programs, clear communication of security policies, and the commitment of top management to prioritize cybersecurity. Furthermore, implementing incident response plans, business continuity management, and conducting regular risk assessments are crucial for effectively responding to and mitigating potential cyber threats. Organizational countermeasures can be divided into four dimensions based on common themes and overlapping objectives of each countermeasure as illustrated in Table 14.

Table 15 shows a ranking of the organizational countermeasures based on their effectiveness and importance. Incident response planning is considered the most effective and important organizational countermeasure for banking and financial services as it helps to ensure a timely and effective response to cybersecurity incidents. Risk management and assessment, security policies and procedures, regular audits and penetration testing, and third-party risk management are also important organizational countermeasures that can help to identify and mitigate cybersecurity risks. Security awareness training, designation of a Chief Information Security Officer (CISO), establishing a Security Operations Center (SOC), employee background checks, threat intelli-

TABLE 14. Dimensions of organizational countermeasures.

Dimension	Description	Example of technical threats
Risk and Incident Management	This dimension focuses on proactive planning and timely response to potential security incidents while managing and mitigating risk	• Incident Response Planning [78], • Risk Management and Assessment [36], • Third-Party Risk Management [53], • Vendor Risk Management [84], • Establishing a Security Operations Center (SOC) [82]
Policy and Governance	This dimension outlines the importance of robust policies, strong leadership, and regular testing to ensure compliance and cybersecurity health	• Security Policies and Procedures [61], • Designation of a Chief Information Security Officer (CISO) [80], • Regular Audits and Penetration Testing [79]
Security Training and Awareness	This dimension focuses on equipping employees with the necessary knowledge to handle cybersecurity threats and emphasizes the importance of personnel security measures and sharing of threat intelligence	• This integrates Security Awareness Training [57], • Employee Background Checks [81], • Threat Intelligence Sharing [83]
Business Continuity and Physical Security	This dimension is centered on ensuring operational resilience in the face of security incidents and protecting physical assets	• Business Continuity and Disaster Recovery (BCDR) Planning [85] • Physical Security [56]

gence sharing, vendor risk management, business continuity and disaster recovery (BCDR) planning, and physical security are also important organizational countermeasures that can help to prevent and detect cyberattacks. Overall, the effectiveness and importance of these organizational countermeasures may vary depending on the specific needs and risks of each organization. Therefore, it is essential for banking and financial services to implement a comprehensive cybersecurity strategy that includes a combination of organizational countermeasures, technical controls, policies, and procedures to mitigate the risks.

VI. LIMITATIONS AND CHALLENGES

While cyber threat classifications provide a valuable framework for understanding and responding to cyber threats in the banking and financial sector, there are several limitations and challenges that must be considered. One limitation is that cyber threats are constantly evolving, and new threats

TABLE 15. Organizational countermeasures.

Organizational Countermeasures	Description
Incident Response Planning [78]	Having a well-defined incident response plan in place allows banks to manage and mitigate the impact of a cyber-attack quickly and effectively.
Risk Management and Assessment [36]	Banks should conduct regular risk assessments to identify potential vulnerabilities and weaknesses in their systems and processes, prioritizing and addressing risks accordingly.
Security Policies and Procedures [61]	Implementing clear and comprehensive security policies and procedures ensures that all employees are aware of their responsibilities regarding cybersecurity and know how to respond to potential threats.
Regular Audits and Penetration Testing [79]	Banks should conduct regular internal and external security audits and penetration tests to identify vulnerabilities in their systems and ensure that security measures are effective.
Third-Party Risk Management [53]	Banks must assess the security posture of third-party vendors and partners, ensuring that they adhere to the same security standards to prevent potential supply chain attacks.
Security Awareness Training [57]	Providing ongoing security awareness training for employees helps them understand the risks and their roles and responsibilities in maintaining cybersecurity, recognize potential threats, and follow best practices.
Designation of a Chief Information Security Officer (CISO) [80]	Assigning a dedicated CISO ensures that there is a senior executive responsible for overseeing cybersecurity strategy and implementation.
Establishing a Security Operations Center (SOC) [82]	An SOC is a centralized unit responsible for monitoring, detecting, and responding to security incidents. A dedicated SOC can significantly enhance an organization's ability to manage and respond to cyber threats.
Employee Background Checks [81]	Conducting thorough background checks on employees, especially those with access to sensitive data or critical systems, can help mitigate the risk of insider threats.
Threat Intelligence Sharing [83]	Banks should participate in industry-specific threat intelligence sharing initiatives, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), to stay informed about the latest threats and vulnerabilities affecting the sector.
Vendor Risk Management [84]	Banks should implement a comprehensive vendor risk management program that evaluates the security posture of third-party vendors and continuously monitors their compliance with security requirements.
Business Continuity and Disaster Recovery (BCDR) Planning [85]	Developing and maintaining BCDR plans ensures that banks can quickly recover from a cyber incident, minimizing downtime and financial losses.
Physical Security [56]	Banks should also consider physical security measures, such as access control systems and surveillance cameras, to prevent unauthorized access to their facilities and the theft or tampering of critical infrastructure.

are emerging all the time. As a result, classifications may become outdated quickly, and organizations must continually update their threat intelligence to stay ahead of attackers. Another challenge is that cyber threats are often interconnected and can occur simultaneously or in quick succession. For example, a cybercriminal may launch a phishing attack to gain access to a financial institution's network and then use that access to launch a ransomware attack. In such cases, the traditional approach of classifying threats in isolation may not be sufficient, and organizations must adopt a more holistic approach to threat management.

Moreover, cyber threat classifications are often based on a range of factors such as the attack vector, the attacker's motivations, and the impact on the organization. However, these factors are not always clear-cut, and cyber-attacks can have multiple motivations and impacts. For example, a cyber-attack on a financial institution may be motivated by financial gain, political reasons, or even revenge. As a result, identifying and classifying the attacker's motivations can be a challenge, and organizations must remain vigilant and adaptable in their response. Finally, there is the challenge of balancing security measures with the need for business operations. In the banking and financial sectors, there are often competing demands between implementing robust security measures and maintaining a seamless customer experience. Striking the right balance requires careful planning and coordination between various stakeholders in the organization. While cyber threat classifications are essential for effective cybersecurity in the banking and financial sector, organizations must also be aware of the limitations and challenges involved. By understanding these challenges and adopting a comprehensive approach to threat management, organizations can better protect themselves and their customers from cyber threats.

VII. CONCLUSION

In this constantly evolving digital age, the banking and financial sector faces an increasingly complex landscape of cyber threats. It is crucial, therefore, that institutions adopt a robust, multi-layered approach to cybersecurity, combining technical controls, legal and regulatory measures, and organizational countermeasures. This will enable them not only to address these threats effectively but also foster a strong culture of security, enhancing their preparedness to tackle and recover from cyber incidents. This approach is key to protecting sensitive data, preserving customer trust, and mitigating financial losses triggered by cyber-attacks. The present research has offered an in-depth exploration of the cyber threats targeting the banking and financial sector and the varied strategies deployed to reduce their risks and impacts. With technology's rapid advancements, the cyber threat landscape continues to shift, spawning new security challenges for the banking industry. Our findings underscore the necessity of a layered approach to cybersecurity that seamlessly integrates technical, legal, and regulatory measures with organizational countermeasures. Collaboration across different stakeholders, continuous vigilance, education of employees, and strategic risk management are pivotal to maintaining a secure operating environment for the banking and financial sector. The insights derived from this research serve as a valuable resource for industry professionals and policymakers to devise more efficacious strategies to counter evolving cyber threats, thereby reinforcing the resilience and security of the sector. This study contributes to the realm of cybersecurity by presenting a comprehensive framework to steer the creation and application of efficient defensive strategies within the banking and financial sectors. The countermeasures identified offer organizations the means to augment their security posture, detect and respond to threats proactively, and minimize the damage ensuing from cyber-attacks. This classification framework stands as a vital tool for practitioners, policymakers, and researchers to identify, prioritize, and mitigate cyber threats within this essential sector. Overall, this research paper provided a comprehensive overview of the cyber threats classification, countermeasures, and challenges faced by the banking and financial sectors. The insights gained from this research can help financial institutions to develop a proactive approach towards cybersecurity and strengthen their resilience against cyber-attacks.

ACKNOWLEDGMENT

The authors gratefully acknowledge the approval and the support of this research study by grant no. (RG-NBU-2022-1724) from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.

REFERENCES

[1] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature," *J. Financial Crime*, vol. 27, no. 3, pp. 945–958, Jun. 2020, doi: 10.1108/JFC-03-2020-0037.

[2] K. Haq, *What is Cybersecurity?* New York, NY, USA: Rosen Education Service, Britannica Educational Publishing, 2018.

[3] Mckinsey.com. (Mar. 10, 2022). *Cybersecurity Trends: Looking Over the Horizon*. Accessed: May 16, 2023. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

[4] Upguard.com. *The 6 Biggest Cyber Threats for Financial Services in 2023*. Accessed: May 16, 2023. [Online]. Available: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services

[5] GuardRails. (Jul. 22, 2022). *The Top 10 Cybersecurity Threats to Digital Banking and how to Guard Against Them*. Accessed: May 16, 2023. [Online]. Available: https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them/

[6] Picussecurity.com. *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*. Accessed: May 16, 2023. [Online]. Available: https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

[7] T. Maurer and A. Nelson, "The global cyber threat," *Finance Develop.*, vol. 1, no. 3, pp. 24–27, 2021.

[8] K. Haq, *What is Cybersecurity?* New York, NY, USA: Rosen Education Service, Britannica Educational Publishing, 2018.

[9] Mckinsey.com. (Mar. 10, 2022). *Cybersecurity Trends: Looking Over the Horizon*. Accessed: May 16, 2023. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

[10] J. Kuepper, "Cyberattacks and the risk of bank failures," Investopedia, (part of the Dotdash Meredith publishing), New York, NY 10007, USA, Jan. 2017. Accessed: May 21, 2023. [Online]. Available: https://www.investopedia.com/articles/personal-finance/012117/cyber-attacks-and-bank-failures-risks-you-should-know.asp

[11] Z. Naz, "Cybersecurity in banking sector: Importance, threats, challenges," Knowledgehut, TX, USA. Accessed: May 21, 2023. [Online]. Available: https://www.knowledgehut.com/blog/security/cyber-security-in-banking
[12] M. N. Dudin and S. V. Shkodinsky, "Challenges and threats of the digital economy to the sustainability of the national banking system," *Finance, Theory Pract.*, vol. 26, no. 6, pp. 52–71, Dec. 2022, doi: 10.26794/2587-5671-2022-26-6-52-71.
[13] N. Goud, "Cyber attacks incur $100 billion losses to financial institutions," Cybersecurity Insiders, Tech. Rep., Jun. 2018. Accessed: May 21, 2023. [Online]. Available: https://www.cybersecurity-insiders.com/cyber-attacks-incur-100-billion-losses-to-financial-institutions/
[14] D. Brando et al., "Implications of cyber risk for financial stability," Board Governors Federal Reserve Syst., FEDS Notes, Washington, DC, USA, May 2022. [Online]. Available: https://doi.org/10.17016/2380-7172.3077
[15] P. Mee and T. Schuermann, "How a cyber attack could cause the next financial crisis," Harvard Business Review, Sep. 14, 2018.
[16] A. I. Al-Alawi and M. S. A. Al-Bassam, "The significance of cybersecurity system in helping managing risk in banking and financial sector," *J. Xidian Univ.*, vol. 14, no. 7, pp. 1523–1536, 2020.
[17] H. M. Alzoubi, T. M. Ghazal, M. K. Hasan, A. Alketbi, R. Kamran, N. A. Al-Dmour, and S. Islam, "Cyber security threats on digital banking," in *Proc. 1st Int. Conf. AI Cybersecurity (ICAIC)*, May 2022, pp. 1–4.
[18] D. Ghelani, T. K. Hua, and S. K. R. Koduru, "Cyber security threats, vulnerabilities, and security solutions models in banking," Authorea, Sep. 2022, doi: 10.22541/au.166385206.63311335/v1.
[19] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers Comput. Sci.*, vol. 3, Mar. 2021, Art. no. 563060.
[20] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature," *J. Financial Crime*, vol. 27, no. 3, pp. 945–958, Jun. 2020.
[21] Z. Barrigar, "Examining the current threat of cybercrime in mobile banking and what can be done to combat it," Ph.D. dissertation, Dept. Cybersecurity, Utica College, Utica Univ., Utica, NY, USA. 2020.
[22] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, Apr. 2019.
[23] M. A. Kazi, S. Woodhead, and D. Gan, "An investigation to detect banking malware network communication traffic using machine learning techniques," *J. Cybersecurity Privacy*, vol. 3, no. 1, pp. 1–23, Dec. 2022.
[24] G. J. W. Kathrine, P. M. Praise, A. A. Rose, and E. C. Kalaivani, "Variants of phishing attacks and their detection techniques," in *Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI)*, Apr. 2019, pp. 255–259.
[25] A. Q. Stanikzai and M. A. Shah, "Evaluation of cyber security threats in banking systems," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Dec. 2021, pp. 1–4.
[26] U. Islam, A. Muhammad, R. Mansoor, M. S. Hossain, I. Ahmad, E. T. Eldin, J. A. Khan, A. U. Rehman, and M. Shafiq, "Detection of distributed denial of service (DDoS) attacks in IoT based monitoring system of banking sector using machine learning models," *Sustainability*, vol. 14, no. 14, p. 8374, Jul. 2022.
[27] S. Yevseiev, K. Rzayev, T. Mammadova, F. Samedov, and N. Romashchenko, "Classification of cyber cruise of informational resources of automated banking systems," *Cybersecurity, Educ., Sci., Technique*, vol. 2, no. 2, pp. 47–67, 2018.
[28] A. Tsvetanova and M. Stefanova, "Key cybersecurity threats," *Math., Comput. Sci. Educ.*, vol. 5, no. 1, pp. 32–38, Dec. 2022, doi: 10.54664/vflf8577.
[29] A. Mukhopadhyay, S. Chatterjee, K. K. Bagchi, P. J. Kirs, and G. K. Shukla, "Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance," *Inf. Syst. Frontiers*, vol. 21, no. 5, pp. 997–1018, Oct. 2019.
[30] Z. Zahoor, M. Ud-din, and K. Sunami, "Challenges in privacy and security in banking sector and related countermeasures," *Int. J. Comput. Appl.*, vol. 144, no. 3, pp. 24–35, Jun. 2016.
[31] V. Wang, H. Nnaji, and J. Jung, "Internet banking in nigeria: Cyber security breaches, practices and capability," *Int. J. Law, Crime Justice*, vol. 62, Sep. 2020, Art. no. 100415.
[32] L. Kaffenberger and E. Kopp, *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment*. Washington, DC, USA: Carnegie Endowment for International Peace, 2019.
[33] B. Sheehan, F. Murphy, A. N. Kia, and R. Kiely, "A quantitative bow-tie cyber risk classification and assessment framework," *J. Risk Res.*, vol. 24, no. 12, pp. 1619–1638, 2021.
[34] A. Bouveret, "Cyber risk for the financial sector: A framework for quantitative assessment," *IMF Work. Papers*, vol. 18, no. 143, p. 1, 2018.
[35] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "The use of the balanced scorecard as a strategic management tool to mitigate cyberfraud in the south African banking industry," *Heliyon*, vol. 8, no. 12, Dec. 2022, Art. no. e12054.
[36] S. Varga, J. Brynielsson, and U. Franke, "Cyber-threat perception and risk management in the Swedish financial sector," *Comput. Secur.*, vol. 105, Jun. 2021, Art. no. 102239.
[37] D. Kiwia, A. Dehghantanha, K.-K.-R. Choo, and J. Slaughter, "A cyber kill chain based taxonomy of banking trojans for evolutionary computational intelligence," *J. Comput. Sci.*, vol. 27, pp. 394–409, Jul. 2018.
[38] B. Vedral, "The vulnerability of the financial system to a systemic cyberattack," in *Proc. 13th Int. Conf. Cyber Conflict (CyCon)*, May 2021, pp. 95–110.
[39] M. Best, L. Krumov, and I. Bacivarov, "Cyber security in banking sector," *Int. J. Inf. Secur. Cybercrime*, vol. 8, no. 2, pp. 39–52, Dec. 2019, doi: 10.19107/ijisc.2019.02.04.
[40] S. Doerr, L. Gambacorta, T. Leach, B. Legros, and D. Whyte, "Cyber risk in central banking," Bank Int. Settlements, Financial Stability Inst., Government Canada, Ottawa, Canada, 2022.
[41] (May 16, 2023). *An Introduction to the Cyber Threat Environment*. [Online]. Available: https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment#defn-compromise
[42] S. Chen, M. Hao, F. Ding, D. Jiang, J. Dong, S. Zhang, Q. Guo, and C. Gao, "Exploring the global geography of cybercrime and its driving forces," *Humanities Social Sci. Commun.*, vol. 10, Feb. 2023, Art. no. 71, doi: 10.1057/s41599-023-01560-x.
[43] R. Mattioli, A. Malatras, E. N. Hunter, M. G. B. Penso, D. Bertram, and I. Neubert, "Identifying emerging cyber security threats and challenges for 2030," Eur. Union Agency Cybersecurity (ENISA), Athens-Heraklion, Greece, Tech. Rep. 64, 2023.
[44] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions," *Electronics*, vol. 11, no. 20, p. 3330, Oct. 2022.
[45] B. Buchanan, "The life cycles of cyber threats," *Survival*, vol. 58, no. 1, pp. 39–58, Jan. 2016.
[46] S. Zhou, Z. Long, L. Tan, and H. Guo, "Automatic identification of indicators of compromise using neural-based sequence labelling," Oct. 2018, *arXiv:1810.10156*.
[47] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, Aug. 2014.
[48] W. Haruna, T. A. Aremu, and Y. A. Modupe, "Defending against cybersecurity threats to the payments and banking system," Dec. 2022, *arXiv:2212.12307*.
[49] O. Shulha, I. Yanenkova, M. Kuzub, I. Muda, and V. Nazarenko, "Banking information resource cybersecurity system modeling," *J. Open Innov., Technol., Market, Complex.*, vol. 8, no. 2, p. 80, Jun. 2022.
[50] P. Weichbroth, K. Wereszko, H. Anacka, and J. Kowal, "Security of cryptocurrencies: A view on the state-of-the-art research and current developments," *Sensors*, vol. 23, no. 6, p. 3155, Mar. 2023, doi: 10.3390/s23063155.
[51] T. C. Helmus, "Artificial intelligence, deepfakes, and disinformation: A primer," Rand Corp., Santa Monica, CA, USA, Tech. Rep. AD1173672, 2022.
[52] M. Lee, "Quantum computing and cybersecurity," Belfer Center Sci. Int. Affairs, Harvard Kennedy School, Cambridge, U.K., Jul. 2021, vol. 7.
[53] O. F. Keskin, K. M. Caramancion, I. Tatar, O. Raza, and U. Tatar, "Cyber third-party risk management: A comparison of non-intrusive risk scoring reports," *Electronics*, vol. 10, no. 10, p. 1168, 2021.
[54] N. Y. Conteh and Q. N. Staton, "The socio-economic impact of identity theft and cybercrime: Preventive measures and solutions," in *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention*. Hershey, PA, USA: IGI Global, 2021, pp. 104–113.
[55] H. F. Atlam and O. Oluwatimilehin, "Business email compromise phishing detection based on machine learning: A systematic literature review," *Electronics*, vol. 12, no. 1, p. 42, Dec. 2022.
[56] R. Badhwar, "Cybersecurity lessons from the breach of physical security at U.S. capitol building," in *The CISO's Transformation*. Cham, Switzerland: Springer, 2021, doi: 10.1007/978-3-030-81412-0_19.

[57] S. E. Kennedy, "The pathway to security – mitigating user negligence," *Inf. Comput. Secur.*, vol. 24, no. 3, pp. 255–264, Jul. 2016.

[58] R. A. M. Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3, no. 1, pp. 1–18, 2020.

[59] S. G. Orr, C. J. Bonyadi, E. Golaszewski, A. T. Sherman, P. A. H. Peterson, R. Forno, S. Johns, and J. Rodriguez, "Shadow IT in higher education: Survey and case study for cybersecurity," *Cryptologia*, pp. 1–65, Oct. 2022.

[60] H. Zamir, "Cybersecurity and social media," in *Cybersecurity for Information Professionals*. Auerbach Publications, 2020, pp. 153–171.

[61] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Comput. Secur.*, vol. 120, Sep. 2022, Art. no. 102820.

[62] A. Henricks and H. Kettani, "On data protection using multi-factor authentication," in *Proc. Int. Conf. Inf. Syst. Syst. Manage.*, Oct. 2019, pp. 1–4.

[63] E. P. Kechagias, G. Chatzistelios, G. A. Papadopoulos, and P. Apostolou, "Digital transformation of the maritime industry: A cybersecurity systemic approach," *Int. J. Crit. Infrastruct. Protection*, vol. 37, Jul. 2022, Art. no. 100526.

[64] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, p. 4759, Jul. 2021.

[65] A. Kamruzzaman, S. Ismat, J. C. Brickley, A. Liu, and K. Thakur, "A comprehensive review of endpoint security: Threats and defenses," in *Proc. Int. Conf. Cyber Warfare Secur. (ICCWS)*, Dec. 2022, pp. 1–7.

[66] N. Basta, M. Ikram, M. A. Kaafar, and A. Walker, "Towards a zero-trust micro-segmentation network security strategy: An evaluation framework," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2022, pp. 1–7.

[67] B. H. Ali, A. A. Jalal, and W. N. I. Al-Obaydy, "Data loss prevention by using MRSH-v2 algorithm," *Int. J. Electr. Comput. Eng.*, vol. 10, pp. 3615–3622, Aug. 2020.

[68] S. Garg, K. Kaur, N. Kumar, and J. J. P. C. Rodrigues, "Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 566–578, Mar. 2019.

[69] D. S. Morozov, T. A. Vakaliuk, A. A. Yefimenko, T. M. Nikitchuk, and R. O. Kolomiiets, "Honeypot and cyber deception as a tool for detecting cyber attacks on critical infrastructure," in *Proc. 3rd Edge Comput. Workshop Doors*, Zhytomyr, Ukraine, Apr. 2023.

[70] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman, and Y. Nam, "Lightweight authenticated-encryption scheme for Internet of Things based on publish-subscribe communication," *IEEE Access*, vol. 8, pp. 60539–60551, 2020.

[71] A. S. Sudarwanto and D. B. B. Kharisma, "Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia," *J. Financial Crime*, vol. 29, no. 4, pp. 1443–1457, Sep. 2022.

[72] P. S. Krüger and J. P. Brauchle, "The European union, cybersecurity, and the financial sector: A primer," Carnegie Endowment Int. Peace Publications Dept., Washington, DC, USA, 2021.

[73] J. C. Crisanto and J. Prenio, "Regulatory approaches to enhance banks' cyber-security frameworks," Bank Int. Settlements, Financial Stability Inst., Basel, Switzerland, Tech. Rep. 2, 2017.

[74] W. Haruna, T. A. Aremu, and Y. A. Modupe, "Defending against cybersecurity threats to the payments and banking system," 2022, *arXiv:2212.12307*.

[75] J. Kosseff, "Defining cybersecurity law," *Iowa Law Rev.*, vol. 103, no. 1, p. 985, 2017.

[76] V. Matejka, J. Soto, and M. Franco, "A framework for the definition and analysis of cyber insurance requirements," M.S. thesis, Commun. Syst. Group, Dept. Inform., Univ. Zurich, Zurich, Switzerland, 2021.

[77] S. Bradshaw, "Combating cyber threats: CSIRTs and fostering international cooperation on cybersecurity," Global Commission Internet Governance Paper Series, Tech. Paper 23, Dec. 2015. [Online]. Available: https://ssrn.com/abstract=2700899 and http://dx.doi.org/10.2139/ssrn.2700899

[78] T. Yohannes, L. Lessa, and S. Negash, "Information security incident response management in an Ethiopian bank: A gap analysis," Addis Ababa Univ. Libraries, Addis Ababa, Ethiopia, 2019.

[79] S. Khattak, S. Jan, I. Ahmad, Z. Wadud, and F. Q. Khan, "An effective security assessment approach for Internet banking services via deep analysis of multimedia data," *Multimedia Syst.*, vol. 27, no. 4, pp. 733–751, Aug. 2021.

[80] E. Karanja, "The role of the chief information security officer in the management of IT security," *Inf. Comput. Secur.*, vol. 25, no. 3, pp. 300–329, 2017.

[81] J. Rushchenko, I. Rushchenko, and O. Plakhova, "Mitigating hiring risks through pre-employment background screening: Methodology based on the personnel security approach," *Technium Social Sci. J.*, vol. 9, pp. 577–587, Jul. 2020.

[82] P. Danquah, "Security operations center: A framework for automated triage, containment and escalation," *J. Inf. Secur.*, vol. 11, no. 4, pp. 225–240, 2020.

[83] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101589.

[84] M. Leo, S. Sharma, and K. Maddulety, "Machine learning in banking risk management: A literature review," *Risks*, vol. 7, no. 1, p. 29, Mar. 2019.

[85] A. Roy, "Analysis of business continuity plan in banking sector," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 8, pp. 982–987, 2022.

[86] A. Ahmad, J. Webb, K. C. Desouza, and J. Boorman, "Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack," *Comput. Secur.*, vol. 86, pp. 402–418, Sep. 2019.

[87] S. Repousis, P. Lois, and V. Veli, "An investigation of the fraud risk and fraud scheme methods in Greek commercial banks," *J. Money Laundering Control*, vol. 22, no. 1, pp. 53–61, Jan. 2019.

[88] D. Javeed and U. MohammedBadamasi, "Man in the middle attacks: Analysis, motivation and prevention," *Int. J. Comput. Netw. Commun. Secur.*, vol. 8, no. 7, pp. 52–58, Jul. 2020.

[89] A. Bani-Hani, M. Majdalweieh, and A. AlShamsi, "Online authentication methods used in banks and attacks against these methods," *Proc. Comput. Sci.*, vol. 151, pp. 1052–1059, Jan. 2019.

[90] K. Thomas, J. Pullman, K. Yeo, A. Raghunathan, P. G. Kelley, L. Invernizzi, B. Benko, T. Pietraszek, S. Patel, D. Boneh, and E. Bursztein, "Protecting accounts from credential stuffing with password breach alerting," in *Proc. USENIX Secur. Symp.*, Aug. 2019, pp. 1556–1571.

[91] A. Sood and R. Enbody, *Targeted Cyber Attacks: Multi-Staged Attacks Driven by Exploits and Malware*. Rockland, MA, USA: Syngress Media, 2014.

[92] I. Tomych. *Cybersecurity in Banking: Main Threats and Challenges in 2023*. Accessed: May 22, 2023. [Online]. Available: https://dashdevs.com/blog/cybersecurity-in-banking-main-threats-and-challenges-in-2023/

[93] *General Data Protection Regulation (GDPR)—Official Legal Text*, Gen. Data Protection Regulation (GDPR). Accessed: May 26, 2023. [Online]. Available: https://gdpr-info.eu/

[94] PCI Compliance Guide. (Mar. 25, 2014). *PCI Compliance Guide Frequently Asked Questions*. Accessed: May 26, 2023. [Online]. Available: https://www.pcicomplianceguide.org/faq/

[95] Financial Crimes Enforcement Network, "Review of bank secrecy act regulations and guidance," *Federal Register*, vol. 86, pp. 71201–71207, Dec-2021.

[96] P. Bukaty, *The California Consumer Privacy Act (CCPA): An Implementation Guide*. IT Governance Publishing, 2019.

[97] I. Alina Boitan, "Cyber security challenges through the lens of financial industry," *Int. J. Appl. Res. Manage. Econ.*, vol. 2, no. 4, pp. 33–38, Jan. 1970.

[98] C. Nobles, "Disrupting the U.S. national security through financial cybercrimes," *Int. J. Hyperconnectivity Internet Things*, vol. 3, no. 1, pp. 1–21, Jan. 2019.

[99] E. Dubois and U. Tatar, "Mitigating global cyber risk through bridging the national incident response capacity gap," in *Proc. Int. Conf. Cyber Warfare Secur.*, Mar. 2022, vol. 17, no. 1, pp. 527–531.

[100] N. Jakovljević, "Analysis of cyber threats as a risk factor in the banking sector," *Bankarstvo*, vol. 51, nos. 3–4, pp. 32–65, 2022.

[101] A. I. Al-Alawi and S. A. Al-Bassam, "Assessing the factors of cybersecurity awareness in the banking sector," *Arab Gulf J. Sci. Res.*, vol. 37, no. 4, pp. 17–32, Dec. 2019.

[102] L. Ali, F. Ali, P. Surendran, and B. Thomas, "The effects of cyber threats on customer's behaviour in e-banking services," *Int. J. e-Educ., e-Bus., e-Manag. e-Learn.*, vol. 7, no. 1, pp. 70–78, 2017.

[103] Z. Lin and Y. Wang, "The impact of technology expenditure on the commercial banks' profitability in Canada," in *Proc. Int. Conf. Econ., Smart Finance Contemp. Trade (ESFCT)*. Canada: Atlantis Press, Dec. 2022, pp. 220–227.

[104] T. Somogyi and R. Nagy, "Cyber threats and security challenges in the Hungarian financial sector," *Contemp. Mil. Challenges/Sodobni vojaški Izzivi*, vol. 24, no. 3, pp. 15–29, 2022.
[105] S. M. Ravitch and M. Riggan, *Reason & Rigor: How Conceptual Frameworks Guide Research*. Newbury Park, CA, USA: Sage, 2016.

ABDULBASIT A. DAREM (Member, IEEE) received the Ph.D. degree in computer science from the University of Mysore, India, in 2014. He is currently an Associate Professor with the Department of Computer Science, Northern Border University, Saudi Arabia. He is a highly accomplished researcher in the field of cyber security. His research has made significant contributions to the development of new methods for detecting and preventing malware attacks. His work has been published in top academic journals and conferences. He has published over 25 papers in top academic journals and conferences. His research interests include cyber security, malware detection, HCI, e-government, and cloud computing. He has received numerous funds and awards for his research excellence.

ASMA A. ALHASHMI received the Ph.D. degree in computer science from the University of Mysore, India, in 2015. She is currently an Assistant Professor with the Department of Computer Science, Northern Border University, Saudi Arabia. She has more than ten years of experience in the IT field. She published more than 17 research papers in reputed international journals and conferences. Her research interests include cybersecurity, software engineering, e-government, and cloud computing.

TAREQ M. ALKHALDI received the Master of Information Technology degree in software engineering from the University of Canberra, Australia, and the Ph.D. degree in information technology from The University of Newcastle, Australia. He was teaching with the College of Computer Science and Information Technology, Department of Artificial Intelligence. He is currently an Assistant Professor with the Department of Educational Technologies, Imam Abdulrahman Bin Faisal University (IAU), Dammam, Saudi Arabia. His research interests include machine learning and data science (big data), intelligent systems, including recommender systems, collaborative filtering and technology-enhanced learning, and IT security.

ABDULLAH M. ALASHJAEE received the Ph.D. degree in computer science from the University of Idaho, USA, in 2021. He is currently an Assistant Professor with the Department of Computer Science, Northern Border University, Saudi Arabia. He has published multiple papers in top academic journals and conferences. His current research focuses specifically on the fields of mobile malware forensics, cybersecurity, digital forensics, and intrusion detection systems.

SULTAN M. ALANAZI received the master's degree in IT and the Ph.D. degree in computer science from the University of Nottingham, U.K. He was a Teaching Assistant with the University of Nottingham. He is currently an Assistant Professor with the Department of Computer Science, Northern Border University, Saudi Arabia. He has more than ten years of experience in the IT field. He published several research papers in reputed international journals and conferences. His research interests include cybersecurity, machine learning, NLP, social network analysis (mining), user modeling, and recommender systems.

SHOUKI A. EBAD received the Ph.D. degree in computer science and engineering from the King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2012. He is currently an Associate Professor with the Department of Computer Science, Faculty of Science, Northern Border University, Saudi Arabia. Before that, he held several positions, such as a Lecturer, the Head of Department, the Vice Dean, an Assistant Dean for Technical Affairs at IT Deanship, and the Secretary of the Scientific Council. He is a Sun Certified Programmer for the Java 2 Platform. His current research interests include software engineering, IT project management, and information security. He published a number of articles in these areas.